AUDIT SISTEM INFORMASI PENELUSURAN PERKARA MENGGUNAKAN *FRAMEWORK* COBIT 5 DAN ITIL V3 2011 (Studi Kasus : Pengadilan Militer II-09 Bandung)

TESIS

Disusun sebagai salah satu syarat untuk
memperoleh gelar Magister Komputer
dari Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Oleh:

WINA NOVIANI FATIMAH

NPM : 2018210006

PROGRAM STUDI PASCA SARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG

2020

AUDIT SISTEM INFORMASI PENELUSURAN PERKARA MENGGUNAKAN *FRAMEWORK* COBIT 5 DAN ITIL V3 2011 (Studi Kasus : Pengadilan Militer II-09 Bandung)

Oleh:

WINA NOVIANI FATIMAH

NPM : 2018210006

Bandung, Januari 2020
Menyetujui,

H. Budi Permana, Dr. S.E., AK., M.SC
Pembimbing

PROGRAM STUDI PASCA SARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG

2020

Dipersembahkan untuk keluarga tercinta

Orangtua, Suami dan Anak

ABSTRAK

Pengadilan Militer II-09 Bandung merupakan salah satu Pengadilan Militer (Dilmil) Tingkat Pertama di Indonesia yang terletak di ibu kota Jawa Barat yaitu Kota Bandung berfungsi menegakkan hukum yang independen, efektif, efisien dan berkeadilan khususnya di lingkungan Tentara Nasional Indonesia (TNI) dan bagi seluruh rakyat Indonesia pada umumnya. Dalam melaksanakan proses bisnis sehari-hari terutama dalam hal proses pengolahan data perkara telah menggunakan teknologi informasi yaitu Sistem Informasi Penelusuran Perkara. COBIT 5 merupakan salah satu kerangka kerja (*framework*) yang bisa digunakan oleh semua jenis organisasi untuk melakukan evaluasi atau audit kinerja pada tata kelola (*governance*) dan manajemen. Pada penerapan layanan Sistem Informasi Penelusuran Perkara terjadi kendala terkait layanan TI yang mempengaruhi data perkara.

Audit Sistem Informasi Penelusuran Perkara menggunakan COBIT 5 yang berfokus pada domain DSS (*Deliver, Service and Support*) yaitu DSS01, DSS02, DSS03, DSS04, DSS05 dan DSS06. Tahapan analisis penelitian menggunakan metode BSC (*Balanced Scorerdcard*) yang direlasikan dengan *Enterprise Golas dan IT-Related Goals* pada COBIT 5. Pengumpulan data berupa observasi, wawancara, kuesioner dan penentuan responden menggunakan RACI *Chart.* Selanjutnya perhitungan hasil kuesioner menggunakan skala *management* dan skala *workproduct* (*output*). selanjutnya dilakukan analisis data dengan menggunakan *capability level* pada COBIT 5 berdasarkan analisis kebutuhan *stakeholder* dengan melakukan pemetaan *Enterprise Goals* ke Tujuan Strategi Pengadilan Militer II-09 Bandung, pemetaan *Enterprise Goals* terhadap *IT-Related Goals,* selanjutnya pemetaan *IT-Related Goals* ke *Processes* pada COBIT 5 sehingga dihasilkan terpilih domain DSS. Setelah dilakukan perhitungan *capability level* dan memiliki nilai GAP. Maka kemudian disusun rekomendasi yang mengacu pada ITIL V3 2011.

Hasil penelitian adalah DSS01 berada *capability level* 2, artinya manajemen kinerja proses dan *output* kinerja pengelolaan operasional telah terkelola dengan baik. DSS02 berada *capability level* 1, artinya permintaan dan layanan insiden telah terdefinisi. DSS03 berada *capability level* 2, artinya manajemen pengelolaan masalah dan *output* kinerja telah sesuai dan memenuhi harapan. DSS04 berada *capability level* 0, artinya proses mengelola kontinuitas gagal dalam mencapai tujuan. DSS05 berada *capability level* 2, artinya manajemen pengelolaan layanan keamanan kinerja proses dan *output* kinerja telah sesuai dan memenuhi harapan dan terkelola dengan baik. DSS06 berada *capability level* 2, artinya manajemen pengelolaan kendala proses bisnis dan *output* kinerja telah sesuai dan memenuhi harapan dan terkelola dengan baik.

Kata kunci : *Audit,* COBIT 5, *DSS (Deliver, Service, and Support), Enterprise Goals*, *IT-Related Goals, RACI Chart,* Skala *Management,* Skala *Workproduct, Capabiliy Level,* ITIL V3 2011

ABSTRACT

Military Court II-09 Bandung is one of the First Level Military Courts (Dilmil) in Indonesia which is located in the capital city of West Java, namely the City of Bandung, which functions to enforce an independent, effective, efficient and just law, especially within the Indonesian National Armed Forces (TNI) and for all Indonesian people in general. In carrying out day-to-day business processes, especially in terms of case data processing, information technology has been used, namely the Case Tracking Information System. COBIT 5 is a framework that can be used by all types of organizations to conduct performance evaluations or audits on governance and management. In the application of Case Search Information System services, there are obstacles related to IT services that affect case data.

Audit Sistem Informasi Penelusuran Perkara uses COBIT 5 which focuses on the DSS (Deliver, Service and Support) domain, namely DSS01, DSS02, DSS03, DSS04, DSS05 and DSS06. Stages of research analysis using the BSC (Balanced Scorerdcard) method which is associated with Enterprise Golas and IT-Related Goals in COBIT 5. Data collection in the form of observation, interviews, questionnaires and determination of respondents using the RACI Chart. Furthermore, the calculation of the results of the questionnaire uses a scale of management and scale of workproduct (output). then performed data analysis using capability level on COBIT 5 based on an analysis of stakeholder needs by mapping Enterprise Goals to the Military Court II-09 Bandung Strategic Objectives, mapping Enterprise Goals to IT-Related Goals, then mapping IT-Related Goals to Processes on COBIT 5 resulting in the chosen DSS domain. After calculating the capability level and GAP value. Then recommendations were made that refer to ITIL V3 2011.

The results of the study are DSS01 at capability level 2, meaning that the process performance management and operational management performance outputs have been well managed. DSS02 is capability level 1, meaning that incident requests and services have been defined. DSS03 is capability level 2, meaning that the management of the problem and the performance output are in line with expectations. DSS04 is capability level 0, meaning that the process of managing continuity fails in achieving its objectives. DSS05 is capability level 2, meaning that the management of security services, process performance and output performance are in line with expectations and are well managed. DSS06 is capability level 2, meaning that the management of business process constraints and performance outputs are in line with expectations and are well managed.

Keywords : Audit, COBIT 5, *DSS (Deliver, Service, and Support), Enterprise Goals*, *IT-Related Goals, RACI Chart,* Skala *Management,* Skala *Workproduct, Capabiliy Level,* ITIL V3 2011

KATA PENGANTAR

Segala puji penulis panjatkan kepada Allah SWT, yang telah memberikan anugerah akal dan pikiran kepada hamba-Nya sehingga penulis dapat menyelesaikan tesis dengan judul *"*Audit Tata Kelola Teknologi Informasi menggunakan *Framework* COBIT 5 dan ITIL V3 2011*"*. Adapun maksud dari pembuatan tesis ini adalah untuk memenuhi salah satu syarat akademik pada kurikulum Strata dua (S-2) Magister Sistem Informasi STMIK LIKMI.

Dalam proses penulisan penelitian ini penulis telah banyak mendapat bantuan, dukungan, dan bimbingan serta doa dari berbagai pihak yang baik terlibat secara langsung maupun tidak langsung. Untuk itu pada kesempatan ini, dengan segala kerendahan hati penulis sampaikan ucapan terima kasih yang setulus-tulusnya kepada :

1. Bapak H. Budi Permana, Dr., S.E., AK., M.Sc., yang selalu memberikan bimbingan dan arahan selama pembuatan tesis ini sehingga dapat diselesaikan dengan baik, semoga Allah S.W.T. membalasnya dengan yang lebih baik. Amin.
2. Kadilmil II-09 Bandung beserta Hakim Militer, Pejabat Struktural dan Staf Pengadilan Militer II-09 Bandung yang telah memperkenankan penulis mengadakan penelitian di tempat tersebut.
3. Orangtua, yaitu Ibu Hj. Lilis Nurjanah, S.Pd.SD dan Bapak H. Kuswara, S.Pd., M.M.Pd yang sepenuhnya mendorong lahir dan bathin untuk penulis menyelesaikan tesis ini.
4. Anak dan Suami, Rayyan Yudhistira Alastar dan Irfan Saepulloh, S.T., M.Kom, yang tidak pernah berhenti mendorong dan menyemangati penulis untuk tetap menyelesaikan kuliah S2 ini.
5. Penulis juga mengucapkan terima kasih kepada seluruh teman kelas S Magister Sistem Informasi angkatan 2018.
6. Staf dan Para Dosen di STMIK LIKMI.

Ucapan terima kasih, disampaikan kepada semua pihak yang tidak dapat disebutkan namanya satu-persatu, yang telah banyak memberikan dukungan, semoga Allah S.W.T. memberikan rahmat, hidayah-Nya serta menggantinya dengan yang lebih baik. Aamiin.

Penulis sadar bahwa penelitian ini masih jauh dari kesempurnaan, oleh karena itu saran dan kritik yang bersifat membangun dari para pembaca sangat penulis harapkan. Akhirnya penulis ucapkan terima kasih kepada semua pihak yang telah membantu kelancaran penyusunan penelitian ini.

Bandung, Desember 2019

Penulis

DAFTAR ISI

KATA PENGANTAR i
DAFTAR ISI iii
DAFTAR TABEL vi
DAFTAR GAMBAR viii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Metodologi Penelitian 4
1.5 Manfaat Penelitian 5
1.6 Ruang Lingkup 5
1.7 Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA 7
2.1 Pengertian Audit Sistem Informasi 7
2.1.1 Tujuan Audit Sistem Informasi 8
2.1.2 Tahapan Audit 9
2.2 Pengertian Sistem Informasi 10
2.3 COBIT (*Control Objectives for Information and related Technology*) 10
2.3.1 Pengertian COBIT 10
2.3.2 COBIT 5 11
2.3.3 Model Referensi Proses COBIT 5 15
2.3.4 Pengukuran Kinerja berdasarkan *Balanced Scoredcard* (BSC) 19
2.3.5 Indikator *Process Assesment Model (*PAM*)* pada COBIT 5 20
2.3.6 Metode Perhitungan Guttman 24
2.4 COBIT 5 Domain DSS (*Deliver, Service, and Support*) 25
2.4.1 DSS01 *Manage Operations* 25
2.4.2 DSS02 *Manage service requests and incidents* 26
2.4.3 DSS03 *Manage problems* 27
2.4.4 DSS04 *Manage continuity* 28
2.4.5 DSS05 *Manage security services* 29
2.4.6 DSS06 *Manage business process* 30
2.5 RACI *Chart* 32
2.6 ITIL (*Information Technology Infrastructure Library*) V3 32
2.6.1 ITIL *Service Design* 37
2.6.2 ITIL *Service Operation* 39
2.7 Pemetaan COBIT 5 dan ITIL V3 2011 41
2.8 Kajian Pustaka 45

BAB III OBJEK DAN METODOLOGI PENELITIAN 50
3.1 Profil Pengadilan Militer II-09 Bandung 50
3.1.1 Visi dan Misi 51
3.1.2 Struktur Organisasi 52
3.1.4 Pemanfaatan Teknologi 54
3.1.5 Infrastruktur 55
3.2 Sistem Informasi Penelusuran Perkara 57
3.3 Metodologi Penellitian 59
3.4 Alur Tahapan Penelitian 59
BAB IV ANALISIS DAN PEMBAHASAN PENELITIAN 64
4.1 Analisis *Stakeholder Drivers* Mempengaruhi Kebutuhan *Stakeholder* 64
4.2 Analisis Kebutuhan *Stakeholder* untuk Tujuan Strategis Pengadilan Militer II-09 Bandung 64
4.3 *Scoring* pada *Enterprise Goals* yang terpilih 71
4.4 Analisis *Enterprise Goals to IT-related Goals* 77
4.5 Pemetaan *IT-Related Goals to processes* 80
4.6 *Scoring* Proses COBIT 5 yang terpilih yaitu DSS 81
4.7 Pengumpulan Data 84
4.8 Pengolahan Data Kuesioner 90
4.8.1 Menghitung Proses dan *Output* DSS01 90
4.8.2 Menghitung Proses dan *Output* DSS02 91
4.8.3 Menghitung Proses dan *Output* DSS03 93
4.8.4 Menghitung Proses dan *Output* DSS04 94
4.8.5 Menghitung Proses dan *Output* DSS05 95
4.8.6 Menghitung Proses dan *Output* DSS06 97
4.9 Penilaian *Capability Level* 99
4.9.1 *Capability Level* proses DSS01 99
4.9.2 *Capability Level* proses DSS02 100
4.9.3 *Capability Level* proses DSS03 102
4.9.4 *Capability Level* proses DSS04 103
4.9.5 C*apability Level* proses DSS05 104
4.9.6 C*apability Level* proses DSS06 106
4.10 Analisis GAP 107
4.11 Pengumpulan Bukti dan Kondisi *Existing* 108
4.12 Rekomendasi 114
BAB V KESIMPULAN DAN SARAN 118
5.1 Kesimpulan 118
5.2 Saran 119

DAFTAR PUSTAKA 120
LAMPIRAN 122

DAFTAR TABEL

Tabel 2.1 Persentase Skala *Rating* 24
Tabel 2.2 Pemetaan COBIT 5 dengan ITIL V3 2011 43
Tabel 2.3 Daftar Penelitian tentang Audit/Evaluasi menggunakan COBIT 5 dan ITIL V3 2011 45
Tabel 3.1 Daftar *Server* dan *Clients* 55
Tabel 3.2 Daftar *Software* resmi dengan lisensi 56
Tabel 4.1 Pemetaan *Enterprise Goals* to Tujuan Strategis (Indikator Tujuan) Pengadilan Militer II-09 Bandung 65
Tabel 4.2 Analisis Keterhubungan *Enterprise Goals* COBIT 5 dengan Tujuan Strategis Pengadilan Militer II-09 Bandung 67
Tabel 4.3 *Enterprise Goals Terpilih* 70
Tabel 4.4 Data Responden *Scoring* pada *Enterprise Goals* yang terpilih 71
Tabel 4.5 *Skala Likert* untuk scoring tingkat kepentingan 72
Tabel 4.6 Rekapitulasi *Scoring* terhadap *Enterprise Goals* 73
Tabel 4.7 Pemetaan *Enterprise Goals* terhadap *IT-Related Goals* 77
Tabel 4.8 Pemetaan *Enterprise-Goals* terhadap *IT-Related Goals* COBIT 5 79
Tabel 4.9 *IT-Related Goals* Terpilih 79
Tabel 4.10 Pemetaan COBIT 5 *IT-Related Goals to Processes* 81
Tabel 4.11 Data Responden pada *Scoring* Proses COBIT 5 yang terpilih yaitu DSS 82
Tabel 4. 12 *Skala Likert* untuk *scoring* tingkat kepentingan 82
Tabel 4. 13 Rekapitulasi *Scoring* COBIT 5 *IT-Related Goals to Processes* 83
Tabel 4.14 Dokumen Pendukung Penelitian 84
Tabel 4.15 Daftar *stakeholder* terkait Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung 86
Tabel 4. 16 Pemetaan Diagram RACI dengan Jabatan dalam struktur organisasi di Pengadilan Militer II-09 Bandung 86
Tabel 4.17 Pemetaan Diagram RACI domain DSS COBIT 5 88
Tabel 4.18 Hasil Pengolahan Data DSS01 pada Level 1 90
Tabel 4.19 Hasil Pengolahan Data DSS02 pada Level 1 92
Tabel 4.20 Hasil Pengolahan Data DSS03 pada Level 1 93
Tabel 4. 21 Hasil Pengolahan Data DSS04 pada Level 1 95
Tabel 4.22 Hasil Pengolahan Data DSS05 pada Level 1 96
Tabel 4.23 Hasil Pengolahan Data DSS06 pada Level 1 98
Tabel 4.24 Pemetaan hasil perhitungan kuesioner DSS01 terhadap *capability level* 1 ... 99
Tabel 4.25 *Capability Level* pada proses DSS01 level 2 99
Tabel 4.26 *Capability Level* pada proses DSS01 level 3 100
Tabel 4.27 Pemetaan hasil perhitungan kuesioner DSS02 terhadap *capability level* 1 . 100

Tabel 4.28 *Capability Level* pada proses DSS02 level 2 101
Tabel 4.29 Pemetaan hasil perhitungan kuesioner DSS03 terhadap *capability level* 1 . 102
Tabel 4.30 *Capability Level* pada proses DSS03 level 2 102
Tabel 4.31 *Capability Level* pada proses DSS03 level 3 103
Tabel 4.32 Pemetaan hasil perhitungan kuesioner DSS04 terhadap *capability level* 1 . 103
Tabel 4.33 Pemetaan hasil perhitungan kuesioner DSS05 terhadap *capability level* 1 . 104
Tabel 4.34 *Capability Level* pada proses DSS05 level 2 105
Tabel 4.35 *Capability Level* pada proses DSS05 level 3 105
Tabel 4.36 Pemetaan hasil perhitungan kuesioner DSS06 terhadap *capability level* 1 . 106
Tabel 4.37 *Capability Level* pada proses DSS06 level 2 107
Tabel 4.38 *Capability Level* pada proses DSS06 level 3 107
Tabel 4.39 Analisis GAP proses DSS 107
Tabel 4.40 Pengumpulan Bukti Proses DSS01 108
Tabel 4.41 Pengumpulan Bukti Proses DSS02 109
Tabel 4.42 Pengumpulan Bukti Proses DSS03 111
Tabel 4.43 Pengumpulan Bukti Proses DSS04 111
Tabel 4.44 Pengumpulan Bukti Proses DSS05 112
Tabel 4.45 Pengumpulan Bukti Proses DSS06 113

DAFTAR GAMBAR

Gambar 2.1 *Business Framework* dari *ISACA* 12
Gambar 2.2 COBIT 5 *Principles* 15
Gambar 2.3 COBIT 5 *Governance dan Management* 19
Gambar 2.4 *Process Assesment Model (PAM)* 21
Gambar 2.5 COBIT 5 *Process Capability Model* 23
Gambar 2.6 *ITIL Lifecycle* 33
Gambar 2.7 Pemetaan COBIT 5 dan ITIL V3 2011 42
Gambar 3.1 Peta Wilayah Hukum Pengadilan Militer II-09 Bandung 51
Gambar 3.2 Struktur Organisasi Pengadilan Militer II-09 Bandung 53
Gambar 3.3 Topologi Jaringan Pengadilan Militer II-09 Bandung 57
Gambar 3.4 Arsitektur Sistem Informasi Penelusuran Perkara 58
Gambar 3.5 Sistem Informasi Penelusuran Perkara Server Lokal 58
Gambar 3.6 Sistem Informasi Penelususran Perkara Server Web 59
Gambar 3.7 Alur Tahapan Penelitian 60

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, perkembangan teknologi informasi tidak dapat terpisahkan dari kegiatan bisnis dan telah menjadi suatu kebutuhan, baik di organisasi swasta atau pemerintah. Peran TI tersebut membantu dalam melakukan pencapaian tujuan yang telah direncanakan serta meningkatkan efektivitas dan efisiensi kinerja. Berdasarkan banyak pengalaman di banyak negara, penggunaan yang terkait teknologi informasi masih menitik beratkan pada upaya-upaya pencatatan eletronik saja. Teknologi informasi belum dioptimalkan dengan maksimal secara progresif dalam meningkatkan kinerja pada badan peradilan. Pada pembangunan dan pengembangan teknologi informasi di Mahkamah Agung diperlukan implementasi pada penggunaan teknologi informasi yang dapat memberikan hasil yang memuaskan dalam pengambilan keputusan serta arah strategis teknologi informasi didalam organisasi peradilan itu sendiri.

Pengaruh peranan teknologi informasi didalam suatu organisasi sangat siginifikan terutama di Peradilan Militer, salah satunya pada membantu pada layanan operasional. Layanan operasional tersebut pada Peradilan Militer berupa layanan keuangan, kepegawaian, adminitrasi umum, dan administrasi perkara. Tugas pokok dan fungsi Peradilan Militer adalah menyelesaikan perkara pidana kejahatan dan pelanggaran terhadap Anggota Militer. Sejak Peradilan Militer bergabung dengan Mahkamah Agung RI pada tahun 2004 berdasarkan Undang-Undang RI No.4 Tahun 2004, penerapan teknologi informasi erat kaitannya dengan proses bisnis pada Peradilan Militer.

Pengadilan Militer II-09 Bandung sebagai salah satu Peradilan Militer di Indonesia yang terletak di Kota Bandung mempunyai tujuan yang hendak dicapai yaitu terwujudnya pelayanan prima bagi masyarakat pencari keadilan dan terwujudnya percepatan proses penanganan perkara melalui pemanfaatan teknologi informasi. Sehingga diharapkan teknologi informasi Sistem Informasi Penelusuran Perkara pada Pengadilan Militer II-09 Bandung dapat meningkat dilihat dari kualitas pelayanan operasional.

Pentingnya audit Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung adalah :

1. Mempertahankan informasi yang berkualitas tinggi untuk mendukung keputusan manajemen.
2. Mencapai tujuan strategis melalui penggunaan TI yang efektif dan efisien.
3. Mengamankan aset sumber daya sistem informasi, termasuk didalamnya adalah aplikasi, data, informasi, infrastruktur (*hardware* dan *software),* manusia beserta perangkat pendukung lainnya.
4. Mencapai keunggulan pada pelayanan operasional melalui penerapan TI yang andal dan efisien.
5. Mempertahankan risiko audit pada tingkat yang dapat diterima (*acceptable audit risk*) jika pada laporan yang terkait TI masih mengandung kesalahan penyajian setelh dilakukan audit.
6. Mengoptimalkan biaya pengelolaan manajemen layanan TI.
7. Mendukung kepatuhan terhadap hukum, peraturan, perjanjian dan kebijakan pengggunaan TI.

Dalam melaksanakan tanggungjawab tersebut serta dalam rangka mewujudkan visi dan misi Pengadilan Militer II-09 Bandung, manajemen harus mengetahui kondisi TI dari instansi, bagaimana pengelolaannya dan pengendaliannya. Dalam pengolahan dan evaluasi teknologi informasi pada layanan operasional dibutuhkan sebuah model pengolahan yang dapat dijadikan sebagai acuan sesuai dengan strategi, visi dan misi Pengadilan Militer II-09 Bandung.

Standar tersebut dapat digunakan sebagai alat pengukuran yang valid dan *reliable*, dan membantu mengatasi permasalahan-permasalahan pada Sistem Informasi Penelusuran Perkara di Pengadilan MIliter II-09 Bandung dengan menggunakan *framework* (kerangka kerja) COBIT 5 (*Control Objectives for Information And Relate Technology*) dan ITIL V3 2011 (*Information Technology Infrastructure Library*). Dalam memetakan tingkat kapabilitas (*capability*) dan manajemen layanan TI tersebut di Pengadilan II-09 Bandung pada saat ini. Pada penelitian ini, acuan kerangka kerja yang

digunakan adalah COBIT 5 dan ITIL V3 2011. Alasan menggunakan kedua *framework* tersebut adalah :

1. COBIT telah menyediakan referensi tentang *best business practice* yang mencakup pada proses bisnis organisasi secara keseluruhan dan mendetailkannya kedalam aktivitas-aktivitas logis yang dapat dikelola dan dikendalikan secara efektif.
2. COBIT dapat digunakan diberbagai jenis organisasi.
3. COBIT 5 merupakan *framework* (kerangka kerja) melakukan pemisahan antara tata kelola (*governance*) dan manajemen (*management*).
4. ITIL menggambarkan *best practice* pada pengelolaan manajemen layanan TI.
5. ITIL menyediakan kerangka kerja yang dapat digunakan pada tata kelola TI dan kualitas untuk perbaikan layanan TI dilihat dari sisi bisnis dan perspektif pengguna (kepuasan pengguna).
6. COBIT dan ITIL memberikan pendekatan yang sifatnya terpadu *top-to-bottom* terhadap tata kelola TI dan manajemen layanan dari perspektif bisnis.
7. COBIT menjelaskan mengenai apa yang harus dilakukan dan ITIL menjelaskan secara rinci bagaimana melakukannya dan menyediakan panduan terhadap kegiatan yang harus dilakukan.
8. Perpaduan antara COBIT dan ITIL akan memperkuat pada tata kelola TI dengan kemungkinan yang lebih besar untuk dukungan manajemen dan penggunaan dan penerapan sumber daya yang lebih efektif.

Alasan penelitian audit Sistem Informasi Penelusuran Perkara yang akan dilaksanakan adalah diharapkan dapat mengetahui kapabilitas (*capability*) dan kesenjangan (*gap*) di Pengadilan Militer II-09 Bandung, sehingga dapat memberikan rekomendasi perbaikan terkait dengan sistem informasi yang sudah dibangun dan penilaian pada domain DSS (*Deliver, Service, Support*) dan layanan TI terutama *delivery service* kepada pengguna sistem informasi di Pengadilan Militer II-09 Bandung.

Berdasarkan uraian diatas, maka penulis akan melakukan penelitian terkait dengan judul “Audit Sistem Informasi Penelusuran Perkara Menggunakan *Framework* COBIT 5 dan ITIL V3 2011 (Studi Kasus : Pengadilan Militer II-09 Bandung)”.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka terdapat beberapa rumusan masalah yang akan dibahas pada penelitian ini, yaitu :

1. Bagaimana keadaan pengelolaan layanan Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung menggunakan kerangka kerja COBIT 5 dan ITIL V3 2011?
2. Bagaimana rekomendasi yang sesuai untuk layanan TI Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung mengacu ke COBIT 5 dan ITIL V3 2011?

1.3 Tujuan Penelitian

Penelitian terkait dengan audit Sistem Informasi Penelusuran Perkara di Pengadilan Mliter II-09 Bandung mempunyai tujuan yaitu :

1. Melakukan analisis dan mengevaluasi pengelolaan layanan TI Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung menggunakan kerangka kerja COBIT 5 dan ITIL V3 2011.
2. Memberikan rekomendasi hasil analisis dan evaluasi terhadap layanan TI Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung.

1.4 Metodologi Penelitian

Metode penelitian yang akan digunakan pada penelitian audit Sistem Informasi Penelusuran Perkara di Pengadilan Mliter II-09 Bandung adalah:

1. Merumuskan masalah.
2. Studi literatur.
3. Pemetaan COBIT 5 dan ITIL V3 2011.
4. Pemilihan domain dan proses yang sesuai dengan penelitian.
5. Melakukan pengumpulan data dan informasi berdasarkan observasi, wawancara dan kuesioner.
6. Mengolah dan menganalisis kuesioner dengan menggunakan standar pada COBIT 5 berdasarkan pada ISO/IEC 15504, yaitu tingkat *capability level* dan analisis *gap.*

7. Memberikan rekomendasi.
8. Kesimpulan dan Saran.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian audit Sistem Informasi Penelusuran Perkara ini adalah:

1. Memperbaiki sektor yang tidak sesuai dengan standar dan manajemen operasional sistem teknologi informasi Sistem Informasi Penelusuran Perkara berdasarkan pengolahan nilai kematangan (*capability*) berdasarkan COBIT 5 dan ITIL V3 2011.
2. Memberikan rekomendasi kepada Pengadilan Militer II-09 Bandung untuk perbaikan layanan TI dengan melakukan penyebaran kuisioner kepada pegawai yang terlibat dalam Sistem Informasi Penelusuran Perkara pada saat proses audit.

1.6 Ruang Lingkup

Penelitian ini difokuskan pada penyelesaian permasalahan layanan TI dengan melakukan audit Sistem Informasi Penelusuran Perkara di Pengadilan Mliter II-09 Bandung pada domain DSS (*Deliver, Service and Support*) COBIT 5 yang berelasi dengan 7 (tujuh) proses di ITIL V3 2011 serta memberikan rekomendasi domain berdasarkan kerangka kerja COBIT 5 dan ITIL V3 2011.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang pelaksanaan, rumusan masalah, tujuan, manfaat dan ruang lingkup penelitian tentang audit sistem informasi penelusuran perkara menggunakan *framework* COBIT 5 dan ITIL V3 2011.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai kajian literatur tentang teori keilmuan yang sesuai dengan audit sistem informasi penelusuran perkara menggunakan *framework* COBIT 5 dan ITIL V3 2011.

BAB III OBJEK DAN METODOLOGI PENELITIAN

Bab ini menyajikan objek penelitian, mekanisme dan teknik atau tatacara bagaimana penelitian mengenai audit sistem informasi penelusuran perkara menggunakan *framework* COBIT 5 dan ITIL V3 2011 dilaksanakan.

BAB IV ANALISIS DAN PEMBAHASAN PENELITIAN

Bab ini berisi mengenai analisis penelitian yang dilaksanakan serta pembahasan terhadap hasill penelitian mengenai audit sistem informasi penelusuran perkara menggunakan *framework* COBIT 5 dan ITIL V3 2011 yang dilaksanakan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang didasarkan pada permasalahan penelitian mengenai audit sistem informasi penelusuran perkara menggunakan *framework* COBIT 5 dan ITIL V3 2011.

BAB II

TINJAUAN PUSTAKA

2.1 Pengertian Audit Sistem Informasi

Berikut ini beberapa pengertian audit dan audit sistem informasi, menurut beberapa ahli yaitu :

1. Pada bukunya Standar Audit Intern Pemerintah (2014:3), AAIPI menjelaskan mengenai:

   Audit adalah proses identifikasi masalah, analisis, dan evaluasi yang dilakukan secara independen, objektif, dan profesional berdasarkan standar audit, untuk menilai kebenaran, kecermatan, kredibilitas, efektivitas, efisiensi, dan keandalan informasi pelaksanaan tugas dan fungsi pemerintah.

2. Menurut Kagerman (2008:2) dalam bukunya *Internal Audit Handbook, Management with the SAP - Audit Roadmap*, menjelaskan :

   In general, auditing is deined as a systematic process of objectively obtaining and evaluating evidence regarding the current condition of an entity, area, process, financial account or control and comparing it to predetermined, accepted criteria and communicating the results to the intended users. he criteria to which the current state is compared may be a legal or regulatory standard (such as the Sarbanes Oxley Act), or internally generated policies and procedures.

3. Menurut Gondodiyoto menjelaskan definisi audit sistem informasi adalah :

   Audit sistem informasi (audit tersendiri dan bukan bagian dari audit laporan keuangan) perlu dilakukan juga untuk memeriksa tingkat kematangan atau kesiapan suatu organisasi dalam melakukan pengelolaan teknologi informasi (IT Governance). (Andry, 2017:2)

4. Menurut ISACA menjelaskan bahwa audit Sistem Informasi adalah :

   Information systems audits can provide a multitude of benefits to an enterprise by ensuring the effective, efficient, secure and reliable operation of the information systems so critical to organizational success.
   (ISACA, 2016)

Dari beberapa pendapat ahli diatas, audit sistem informasi adalah proses sistematis yang secara objektif mengidentifikasi masalah, menganalisis, dan mengevaluasi bukti mengenai kondisi terkini suatu entitas, area, proses, akun keuangan, atau kontrol dari suatu organisasi apakah suatu sistem aplikasi yang terkomputerisasi dan pengelolaan teknologi informasi telah menerapkan pengendalian intern dan membandingkannya

dengan kriteria yang telah ditentukan audit sistem informasi memberikan banyak manfaat bagi organisasi.

2.1.1 Tujuan Audit Sistem Informasi

Dilihat dari beberapa definisi tersebut diatas, maka dapat disimpulkan bahwa tujuan audit sistem informasi menurut Gondodiyoto (Andry, 2017:2) adalah untuk melakukan penilaian terhadap pengendalian sistem informasi apakah telah dapat memberikan keyakinan memadai atas :

1. Pengamanan aset

   Aset informasi yang ada pada suatu organisasi yaitu berupa *hardware* (perangkat keras), *software* (perangkat lunak), sumber daya manusia, *file/data* dan fasilitas lainnya yang harus dijaga dengan melakukan pengendalian internal secara baik supaya tidak terjadi suatu penyalahgunaan aset di organisasi tersebut.

2. Efektivitas sistem

   Efektivitas sistem informasi dalam suatu organisasi memiliki peranan yang sangat penting pada pengambilan keputusan. Sistem informasi dikatakan efektif adalah jika sistem telah dirancang dengan benar dan disesuaikan dengan kebutuah *user.*

3. Efisiensi sistem

   Sumber daya suatu waktu kapasitasnya akan terbatas maka dibutuhkan efisiensi. Jika kinerja dari sistem aplikasi di komputer telah menurun selanjutnya pihak manajemen perlu melakukan evaluasi tentang efisiensi sistem, apakah sistem informasi telah memadai atau organisasi harus menambah terkait sumber daya yang baru. Sistem disebut telah efisiensi jika telah memenuhi kebutuhan pengguna (*user)* dengan sumber daya informasi.

4. Ketersediaan (*availability*)

   Ketersediaan dukungan/layanan TI hendaknya kontributif terhadap berkelanjutan kegiatan proses bisnis organisasi.

5. Kerahasiaan (*confidentiality*)

   Kerahasiaan berfokus pada perlindungan terhadap informasi agar terhindar dari akses pihak-pihak yang tidak bertanggungjawab.

6. Kehandalan (*reliability*)

   Kehandalan yaitu yang berhubungan dengan kesesuaian dan keakuratan data dan informasi untuk pihak manajemen dalam melakukan pengelolaan organisasi, pembuatan pelaporan dan pertanggungjawaban.

7. Menjaga integritas data (*data integrity*)

   Integritas data merupakan konsep dasar sistem informasi dimana data mempunyai atribut-atribut kelengkapan yaitu kebenaran, dan keakuratan.

2.1.2 Tahapan Audit

Pada buku *Audit and Control of Information System*, menurut Senft (2013), terdapat beberapa tahapan proses audit sistem informasi, yaitu :

1. Perencanaan (*Plannning*)

   Tahapan perencanaan awal mula dari pelaksanaan audit maka mutlak perlu dilakukan untuk mengenal baik dan benar mengenai objek audit yang akan dilkukan pemeriksaan dan memastikan bahwa sumber daya sudah dimiliki. Selanjutnya pelaksanaan audit dikatakan akan berjalan efektif dan efisien, karena dilakukan oleh orang-orang yang mempunyai kompetensi dibidangnya, serta dapat diselesaikan secara tepat waktu sesuai dengan kesepakatan.

2. Pemeriksaan Lapangan (*Fieldwork*)

   Pada tahapan ini dilakukan pengumpulan bukti-bukti yang terkait dan memadai dengan berbagai Teknik yaitu survey, wawancara, observasi dan review dokumentasi.

3. Pelaporan (*Reporting*)

   Pada tahap ini mulai dikembangkan terkait temuan-temuan audit, kemudian menggabungkan temuan-temuan tersebut ke dalam sebuah laporan yang logis, selanjutnya menyiapkan bukti-bukti terkait sebagai alat pendukung dan dokumentasi sesuai dengan yang diperlukan pada saat tindak lanjut.

4. Tindak lanjut (*"Follow Up*)

   Melakukan evaluasi dari berbagai informasi yang relevan dan memastikan tindak lanjut dari temuan telah dilaksanakan oleh pihak manajemen tepat pada waktunya.

2.2 Pengertian Sistem Informasi

Keberlangsungan operasional sebuah organisasi tidak akan pernah lepas dari peran sistem informasi yang dimiliki didalam internal organisasi. Dibawah akan dijelaskan pengertian sistem informasi menurut ahli-ahli, yaitu sebagai berikut :

1. Menurut Romney dan Steinbart (2015:3-4) dalam bukunya *Accounting Information Systems Thirtheenth Edition* :

   System is is a set of two or more interrelated components that interact to achieve a goal. Most systems are composed of smaller subsystems that support the larger system. Data are facts that are collected, recorded, stored, and processed by an information system. Information is data that have been organized and processed to provide meaning and improve the decision-making process.

2. Sedangkan menurut Laudon pada buku *Management Information* Systems :

   An information system can be defined technically as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization.
   (Laudon, 2014:45)

3. Pada buku *Systems Analysis and Design Methods Seventh Edition* menurut Whitten dan Bentley :

   Information System (IS) an arrangement of people, data, processes, and information technology that interact to collect, process, store, and provide as output the information needed to support an organization.
   (Whitten, 2007:6)

Dapat disimpulkan bahwa sistem informasi adalah kumpulan komponen-komponen yang mempunyai keterkaitan satu sama lain dengan tujuan mengumpulkan, memproses, menyimpan, dan menghasilkan informasi dalam mendukung keputusan atau pengendalian pada suatu organisasi.

2.3 COBIT (*Control Objectives for Information and related Technology*)

COBIT mempunyai bertujuan menyediakan manajemen dan pemilik dari proses bisnis dengan model tata kelola TI yang membantu dalam memberikan nilai TI, memahami dan mengelola risiko terkait dengan TI.

2.3.1 Pengertian COBIT

COBIT diterbitkan pertama kali oleh ISACA (*Information System Audit and Control Association*) dengan tujuan untuk membantu memenuhi berbagai kebutuhan oleh manajemen terhadap informasi dengan menjembatani kesenjangan (*gap*) antara

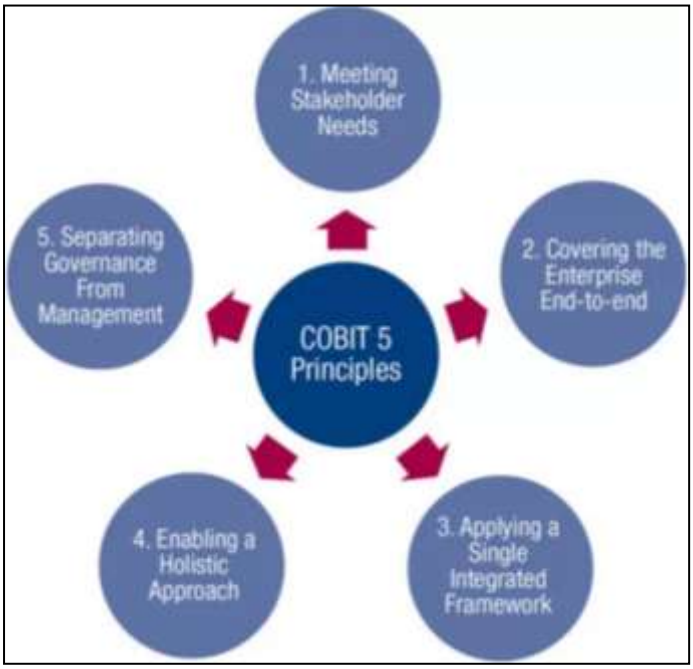
kebutuhan yang dikendalikan (*control requirements*), masalah teknis (*technical issues*) dan risiko bisnis (*business risk*) dan menjaga keseimbangan antara manfaat dengan risiko yang diperoleh dengan mengoptimalkan penggunaan sumber daya TI. (ISACA, 2012)

Pengembangan kerangka kerja (*framework*) COBIT sebagai *best practice* untuk memberikan metode dasar pada penataan dan pelaksanaan audit *IT Governance* (tata kelola TI). Kerangka kerja COBIT telah mendapat pengakuan di seluruh dunia sebagai alat atau standar yang paling efektif dan dapat diandalkan untuk implementasi dan audit pada tata kelola TI, serta untuk melakukan penilaian terhadap kemampuan TI.

Kerangka kerja COBIT merespon agar berhasil dan akan sejalan dengan bisnis, manajemen harus menerapkan sistem pengendalian internal atau membuat hubungan antara kebutuhan kerangka kerja dengan persyaratan bisnis, mengorganisir kegiatan TI menjadi proses melalui model proses yang akan diterima secara luas, mengidentifikasi pemanfaatan sumber daya TI yang paling penting, menentukan pertimbangan tujuan dari pengendalian. Kerangka kerja COBIT dibuat dengan karakteristik utama, yaitu : *Business-focused* (Fokus bisnis)*, Process-oriented* (Orientasi proses)*, Control-based* (dasar pengendalian)*, Measurement-driven*. Kerangka kerja COBIT juga mengidentifikasi mana dari tujuh kriteria informasi *effectiveness* (efektivitas)*, efficiency* (efisiensi)*, confidentiality* (kerahasiaan)*, integrity* (integritas)*, availability* (ketersediaan)*, compliance* (kepatuhan) *and reliability (*keandalan*)*. COBIT mengkategorikan kegiatan TI ke dalam model proses umum yang terdiri dari 4 (empat) domain utama, yaitu *Plan and Organize* (PO), *Acquire and Implement* (AI), *Deliver, Service and Support* (DSS), *Monitor and Evaluate* (ME).

2.3.2 COBIT 5

COBIT 5 adalah pengembangan dari COBIT 4.1 sebagai salah satu *framework* (kerangka kerja) yang digunakan untuk melakukan proses audit. COBIT dinilai sebagai standar yang lengkap dan menyeluruh sebagai *framework* audit dan dapat digunakan semua jenis organisasi. C Berikut ini gambar 2.2 adalah 5 (lima) prinsip pada *framework* COBIT 5.



Gambar 2.1
COBIT 5 *Principles* (ISACA, 2012)

COBIT 5 dibangun dari 5 prinsip-prinsip utama berdasarkan (ISACA, 2012:14) yang diilustrasikan pada gambar 2.1 tersebut diatas. Prinsip-prinsip pada COBIT 5 yaitu :

1. *Meeting stakeholders needs*

   Organisasi hadir dalam menciptakan nilai bagi *stakeholders* (para pemangku kepentingan) yaitu menjaga keseimbangan antara pencapaian manfaat dan optimalisasi terhadap risiko dan penggunaan pada sumber daya. COBIT 5 menyediakan panduan tentang semua proses yang diperlukan dan pendukung lainnya melalui penggunan TI untuk menciptakan nilai bisnis. Berbagai organisasi mempunyai tujuan yang berbeda-beda, COBIT 5 menyediakan *Goals Cascade*, menerjemahkan sasaran organisasi tingkat tinggi menjadi tujuan yang dapat dikelola secara spesifik terkait TI dan memetakannya ke proses dan praktik tertentu. Langkah-langkah *Goals Cascade* pada COBIT 5 adalah :

   a. Langkah-1 *Stakeholder Drivers Influence Stakeholder Needs*

      Kebutuhan pemangku kepentingan dipengaruhi oleh sejumlah pemicu.

      Misalnya perubahan strategi, lingkungan bisnis dan peraturan yang berubah, dan teknologi baru.

b. Langkah-2 *Stakeholder Needs Cascade to Enterprise Goals*

Kebutuhan pemangku kepentingan dapat dikaitkan dengan serangkaian tujuan umum organisasi. Sasaran-sasaran organisasi telah dikembangkan dengan menggunakan BSC (*Balanced Scorecard*).

c. Langkah-3 *Enterprise Goals Cascade to IT-related Goals*

Terkait proses pencapaian tujuan pada organisasi dibutuhkan sejumlah hasil dari *IT-related*, hal tersebut direpresentasikan oleh *IT-related Goals*. *IT-related* merupakan singkatan yang artinya adalah terkait informasi dan teknologi, dan *IT-related Goals* disusun dengan dimensi *IT Balanced Scorecard* (IT BSC).

d. Langkah-4 *IT-related Goals Cascade to Enabler Goals*

Dalam mencapai *IT-related Goals* dibutuhkan aplikasi dan menggunakan sejumlah *enabler.* Yang diisebut e*nabler* adalah proses, struktur organisasi, dan informasi dan dan untuk masing-masing *enabler* merupakan serangkaian tujuan spesifik yang relevan dan didefinisikan untuk mendukung *IT-related Goals*.

2. *Covering the enterprise end-to-end*

COBIT 5 mengintegrasikan tata kelola TI menjadi bagian yang tidak terpisah dari tata kelola organisasi.

a. Pada COBIT 5 fungsi dan proses pada organisasi tidak berfokus pada fungsi TI saja, melainkan TI diperlakukan sebagai aset yang perlu diperlakukan dan ditangani seperti halnya aset lain di organisasi.

b. Menganggap semua pemberdayaan tata kelola dan manajemen TI untuk menjadi organisasi dan *end-to-end*.

3. *Applying a single integrated framework*

Sebagai *best practice* kegiatan TI yang sejalan dengan standar atau panduan kerangka kerja lain yang relevan di tingkat tinggi, dan berfungsi menyeluruh untuk *governance* dan *management* TI di organisasi.

4. *Enabling a Holistic Approach*

Tata kelola dan manajemen TI yang efektif dan efisien membutuhkan terkait pendekatan holistik yang mempertimbangkan terhadap komponen-komponen yang

memiliki interaksi. COBIT 5 menjelaskan seperangkat *enabler* dalam rangka mendukung proses implementasi sistem tata kelola dan manajemen TI secara komprehensif untuk organisasi. *Enabler* merupakan segala sesuatu yang membantu dalam mencapai tujuan organisasi. Kerangka kerja COBIT 5 (ISACA, 2012:31) mendefinisikan tujuh kategori *enabler*, yaitu :

a. Prinsip-prisnip, Kebijakan dan Kerangka kerja

   Kendaraan dimana keputusan tata kelola dilembagakan dalam organisasi, dengan alasan interaksi antara keputusan tata kelola sebagai pengaturan arah dan manajemen sebagai pelaksanaan keputusan.

b. Proses

   Dalam model proses COBIT 5, dibuat perbedaan masing-masing antara rangkaian praktik dan kegiatan tata kelola dan proses manajemen. Model proses juga termasuk grafik RACI, menggambarkan tanggung jawab dan peran dalam struktur organisasi pada organisasi.

c. Struktur Organisasi

   Struktur organisasi terdapat pada ruang tata kelola atau ruang manajemen, tergantung pada komposisi dan ruang lingkup keputusan pada organisasi tersebut.

d. Budaya, Prilaku dan Etika

   Perilaku sebagai pendukung utama pada tata kelola dan manajemen di organisasi yang dikelola dengan baik.

e. Informasi

   Model proses menggambarkan *input* dan *output* dari sebuah proses ke proses lain, termasuk pertukaran informasi antara tata kelola dan proses manajemen. Informasi digunakan untuk mengevaluasi, mengarahkan dan memantau organisasi TI antara tata kelola dan manajemen.

f. Layanan, Infrastruktur dan Aplikasi

   Layanan diperlukan dan didukung oleh aplikasi dan infrastruktur dengan tujuan memberikan informasi memadai kepada badan tata kelola untuk mendukung,

evaluasi, menetapkan arah dan memantau kegiatan tata kelola.

g. Orang, Keterampilan dan Kompetensi

Kegiatan tata kelola dan manajemen membutuhkan rangkaian keterampilan yang berbeda, bagi anggota badan tata kelola dan manajemen.

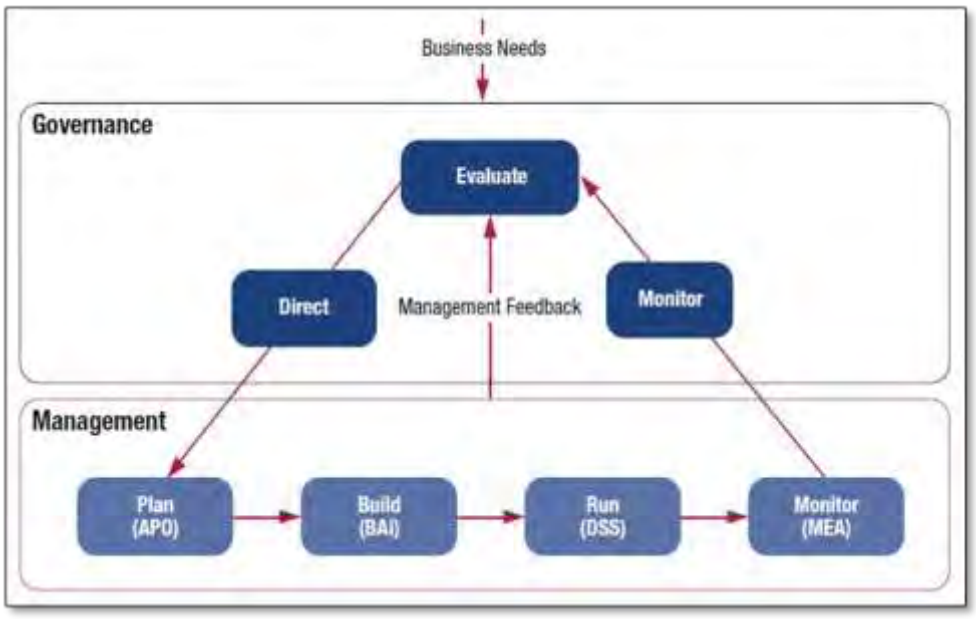
5. *Separating Governance from Management*

COBIT 5 membedakan secara jelas antara tata kelola dan manajemen seperti yang terlihat pada gambar 2.2

2.3.3 Model Referensi Proses COBIT 5

COBIT 5 menganjurkan agar perusahaan menerapkan tata kelola dan proses manajemen yang dapat mencakup bidang-bidang utama. Model referensi proses pada COBIT 5 mendefinisikan serta menjelaskan secara rinci sejumlah proses tata kelola dan manajemen. Itu digambarkan mewakili semua proses di organisasi yang berkaitan dengan TI yang dapat dimengerti oleh operasional TI dan manajer bisnis.

Model Referensi Proses COBIT 5 dibagi menjadi Tata Kelola (*Governance)* dan Manajemen (*Management)* (ISACA, 2012:14) menjadi dua domain proses, yaitu :



Gambar 2.2
Model Referensi pada COBIT 5 (ISACA, 2012:32)

1. Tata Kelola (*Governance)*

Menurut (ISACA, 2012:14) *Gorvernance* (Tata kelola) melakukan evaluasi ter-

hadap kebutuhan, kondisi, dan pilihan pemangku kepentingan dengan tujuan untuk menentukan keseimbangan, kesepakatan tujuan organisasi untuk dicapai; menetapkan arah melalui penentuan prioritas bisnis, pengambilan keputusan; dan melakukan pemantauan kinerja serta ketaatan terhadap arah dan tujuan yang telah disepakati.

Governance berisi lima proses tata kelola, dalam setiap proses *Evaluate, Direct* dan *Monitor* (EDM) (ISACA, 2012:32). Proses-proses EDM, yaitu :

a. EDM01 *Ensure governance framework setting and maintenance*
b. EDM02 *Ensure benefits delivery*
c. EDM03 *Ensure risk optimation*
d. EDM04 *Ensure resource optimasion*
e. EDM05 *Ensure stakeholder transparancy*

2. Manajemen *(Management)*

Rencana manajemen adalah membangun, menjalankan dan memantau kegiatan yang sejalan dengan arahan yang telah ditetapkan dalam mencapai tujuan organisasi.

Pada domain manajemen terdiri dari 4 proses yaitu merencanakan (*Plans),* membangun *(Builds),* menjalankan (*Runs),* dan memantau (*Monitors).* Berikut ini adalah domain yang ada pada manajemen yaitu sebagai berikut :

a. *Align, Plan and Organise* (APO)

Menyediakan panduan untuk *solution delivery* dan *service delivery* (BAI) serta pendukung (DSS). Domain ini strategi dan cara, dan mengidentifikasi dengan cara terbaik TI dapat yang berandil dalam melakukan pencapaian tujuan bisnis. Proses-proses pada APO yaitu :

1) APO01 *Manage The IT management Framework*
2) APO02 *Manage Strategy*
3) APO03 *Manage Enterprise architecture*
4) APO04 *Manage innovation*
5) APO05 *Manage portfolio*

6) APO06 *Manage budget and costs*

7) APO07 *Manage human resources*

8) APO08 *Manage relationship*

9) APO09 *Manage service agreement*

10) APO10 *Manage suppliers*

11) APO11 *Manage quality*

12) APO12 *Manage risk*

13) APO13 *Manage security*

b. *Build, Aquire and Implement* (BAI)

Menyediakan solusi dan mengantarkannya dalam sebuah layanan. Tujuan domain BAI adalah untuk merealisasikan strategi TI, mengidentifikasi solusi TI yang dikembangkan dan diperoleh, serta mengimpelentasikan dan mengintegrasikan ke dalam proses bisnis. Domain ini juga meliputi perubahan dalam proses *manitenance* sistem, dan menjamin bahwa solusi TI dapat secara terus menerus memenuhi tujuan bisnis.

Proses-proses BAI terdiri dari :

1) BAI01 *Manage programmes and projects*

2) BAI02 *Manage requirements and definitions*

3) BAI03 *Manage solutions identification and build*

4) BAI04 *Manage availability adn capacity*

5) BAI05 *Manage organisational change enablement*

6) BAI06 *Manage changes*

7) BAI07 *Manage change acceptance and transitioning*

8) BAI08 *Manage knowledge*

9) BAI09 *Manage assets*

10) BAI10 *Manage configuration*

c. *Deliver, Service and Support* (DSS)

Domain ini berfokus pada bagaimana penerimaan solusi dan kegunaannya dalam membantu *user*, pengantaran dan dukungan dari layanan yang

dibutuhkan, termasuk di dalamnya pengantaran nilai, manajemen keamanan, layanan pendukung untuk *user* serta manajemen data dan fasilitas-fasilitas operasional.

Proses-proses DSS sebagai berikut :

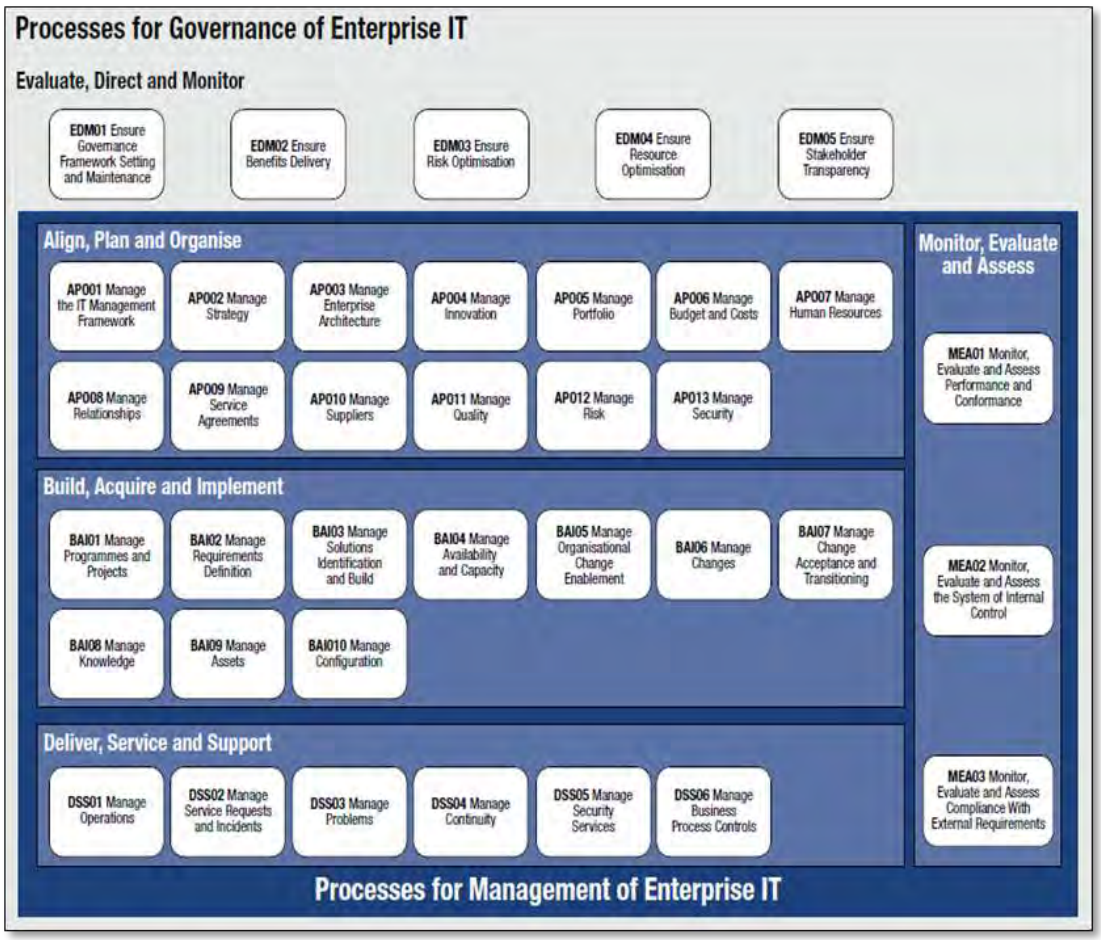
1) DSS01 *Manage opreations*
2) DSS02 *Manage service requests and incidents*
3) DSS03 *Manage problems*
4) DSS04 *Manage continuity*
5) DSS05 *Manage security services*
6) DSS06 *Manage business process control*

d. *Monitor, Evaluate and Assess* (MEA)

Melakukan pengawasan terhadap semua proses yang menjamin bahwa arahan/panduan dijalankan dengan benar. Semua proses TI harus sering diukur untuk mengetahui kualitas serta pemenuhannya dengan sebuah pengendalian kebutuhan.

1) MEA01 *Monitor, evaluate and assess performance and conformance*
2) MEA02 *Monitor, evaluate and assess the system of internal control*
3) MEA03 *Monitor, evaluate and assess compliance with external requirements*

Gambar 2.3 (ISACA, 2012:33) menunjukkan set lengkap 37 dalam COBIT 5. Detail dari semua proses, sesuai dengan model proses yang dijelaskan sebelumnya, termasuk dalam COBIT 5 : *Enabling Processes*



Gambar 2.3
The COBIT 5 *process reference model* (PRM) (ISACA, 2012:33)

Pengelolaan TI menjadi kebutuhan yang sangat siginifikan bagi organisasi yang menggunakan TI sebagai dasar proses kerja organisasi tersebut. Berdasarkan standar COBIT 5, pengelolaan kebutuhan TI mempunyai tujuan dalam menjaga keseimbangan antara melakukan realisasi kelebihan dan melakukan pengoptimalan tingkat risiko dan penggunaan terhadap sumber daya, yang dapat menunjang untuk proses kinerja dan kegiatan bisnis pada organisasi dengan menggunakan teknologi informasi.

2.3.4 Pengukuran Kinerja berdasarkan *Balanced Scoredcard* (BSC)

Balanced Scorecard merupakan metode terhadap pengukuran kinerja secara komprehensif yang menterjemahkan visi dan misi serta sasaran strategis organisasi dalam satu ruang lingkup ukuran kinerja yang terpadu, yang tersusun dari 4 (empat) perspektif yaitu *Financial, Customer*, *Internal Business Process*, dan *Learning and Growth.* (Pertiwi, 2014:1)

Maka *Balanced Scorecard* sering disingkat BSC merupakan alat ukur kinerja yang mengukur kinerja perusahaan atau organisasi secara keseluruhan, baik dari secara keuangan atau non-keuangan yang dilihat dari 4 (empat) perspektif yang tersebut diatas, serta memberikan kerangka berpikir untuk menjabarkan strategi organisasi ke dalam layanan operasional, kemudian menciptkan nilai terhadap pelanggan pada sat ini dan masa mendatang. Hal tersebut termasuk bagaimana cara perusahaan atau organisasi meningkatkan kemampuan internal yaitu investasi pada manusia, sistem, prosedur yang dibutuhkan untuk mengetahui kinerja yang lebih baik dimasa mendatang. Perspektif *Balanced Scorecard* yaitu :

1. *Financial*

   Perspektif keuangan menunjukkan antara perencanaan dan pelaksanaan strategi organisasi apakah memberikan perbaikan atau peningkatan keuntungan organisasi.

2. *Customer*

   Perspektif pelanggan menunjukkan peningkatan terhadap pengakuan atas pentingnya pelanggan .

3. *Internal Business Process*

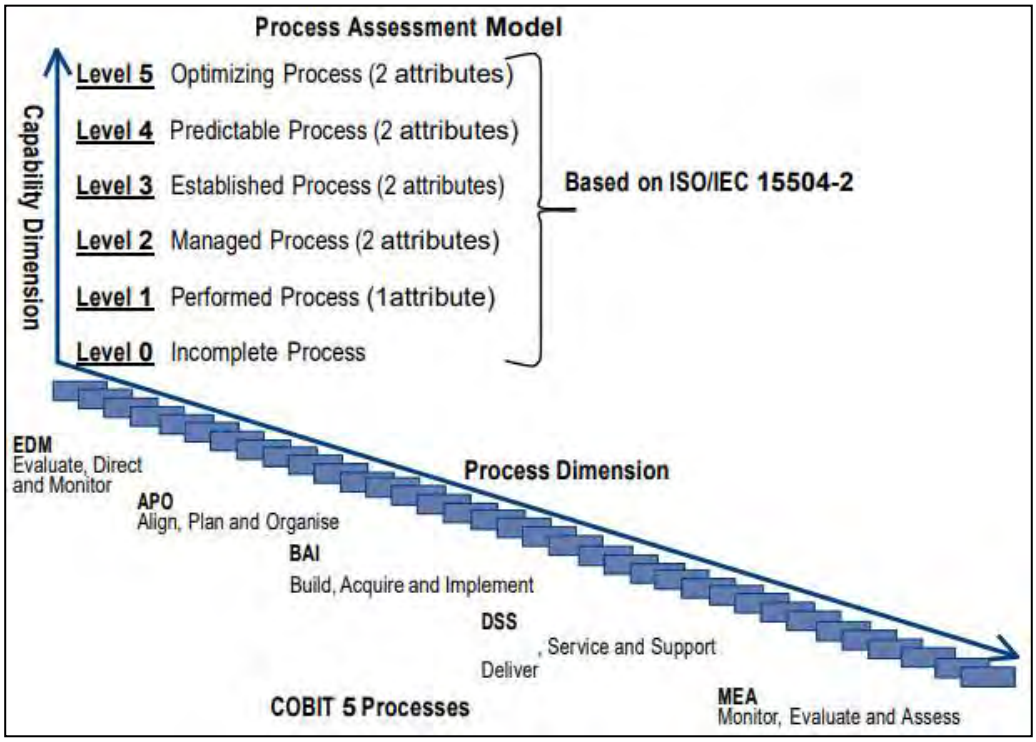
   Perspektif proses bisnis internal mengidentifikasi proses bisnis internal pada organisasi yang bersifat kritis dan harus diunggulkan oleh organisasi.

4. *Learning and Growth*

   Mengidentifikasi infrastruktur yang harus dibangun oleh organisasi atau perusahaan untuk meningkatkan pertumbuhan dan kinerja dalam jangka panjang.

2.3.5 Indikator *Process Assesment Model (*PAM*)* pada COBIT 5

Process Assesment Model (PAM) adalah sebuah model kapabilitas proses dua dimensi seperti pada Gambar 2.4



Gambar 2.4
Process Assesment Model (PAM) (ISACA, 2012:11)

Proses TI pada COBIT 5 dapat dilakukan penilaian berdasarkan tingat kematangannya dengan menggunakan *Capability Level*. *Capability Level* yang terdiri dari 6 (enam) level yaitu level 0 (*Incomplete)* sampai level 5 (*Optimised*) (ISACA, 2012:13). Keenam level tersebut adalah:

1. Level 0: *Incomplete Process.* Pada tahap ini organisasi tidak melaksanakan proses-proses TI.
2. Level 1: *Performed Process.* Pada tahap ini organisasi telah melaksanakan secara berhasil terhadap proses dan tujuan TI telah benar-benar tercapai.
    - PA 1.1 melakukan pengukuran sejauh mana tujuan proses yang dilaksanakan telah dicapai. Hasil dari pencapaian dari atribut ini akan tercermin dari setiap proses yang menghasilkan *output* yang diharapkan.
3. Level 2: *Managed Process.* Pada tahap ini organisasi pada saat melaksanakan proses TI untuk mencapai tujuannya dilaksanakan dengan baik dan secara terkelola. Pengelolaan tersebut dimulai dari proses perencanaan, selanjutnya evaluasi dan penyesuaian terhadap arah yang lebih baik lagi. Atribut pada level ini adalah :

a. PA 2.1 *Performance Management* mengukur sampai sejauh mana pelaksanaan proses disusun dengan baik.

b. PA 2.2 *Work Product Manamgement* mengukur sejauh mana produk kerja yang telah diproduksi oleh proses setelah diatur dengan baik.

5. Level 3: *Established Process.* Pada tahap ini organisasi mempunyai proses-proses TI yang telah terstandar secara keseluruhan di organisasi.

   a. PA 3.1 *Process Definition* mengukur sejauh mana proses didefinisikan untuk mendukung terhadap pelaksanaan proses.

   b. PA 3.2 *Process Deployment* mengukur sejauh mana standar proses dilaksanakan secara efektif.

6. Level 4: *Predictable Process.* Pada tahap ini organisasi telah menjalankan terkait proses TI pada batasan-batasan yang telah pasti. Batasan ini didapatkan dari pelaksanaan kegiatan pengukuran yang telah dilaksanakan saat proses TI pada tahap sebelumnya.

   a. PA 4.1 *Process Measurment* mengukur sejauh mana hasil dari pengukuran yang digunakan untuk menjamin pelaksanaan proses sehingga mendukung hasil capaian tujuan organisasi.

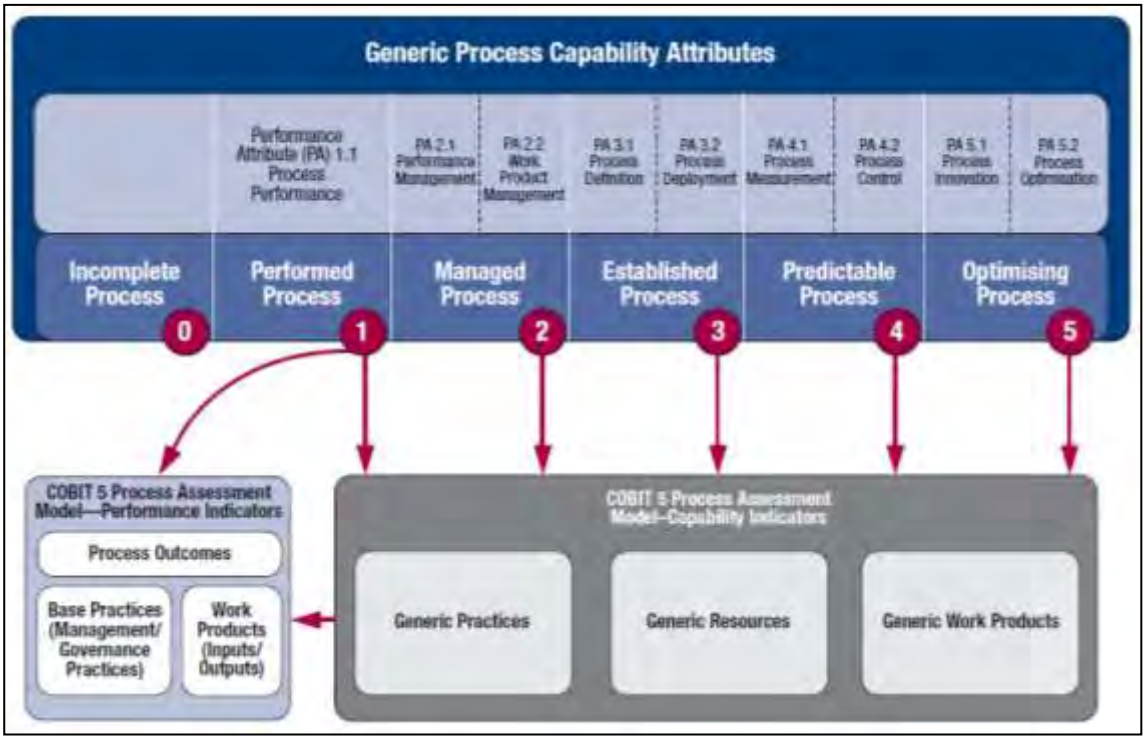
   b. PA 4.2 *Process Control* mengukur sejauh mana proses yang telah disusun secara kualitatif sehingga menghasilkan proses yang stabil/tetap dan bisa diprediksi sesuai dengan batasan yang telah didefinisikan.

7. Level 5: *Optimizing Process P*ada tahap ini organisasi telah melaksanakan proses inovasi-inovasi dan telah melaksanakann perbaikan yang berkesinambungan agar meningkatkan kemampuannya.

   a. PA 5.1 *Process Inovation* melakukan pengukuran terhadap perubahan proses yang teridentifikasi dari pelaksanaan proses dari pendekatan inovasi terhadap pelaksanaan proses.

   b. PA 5.2 *Process Optimation* melakukan pengukuran pada sejauh mana perubah-

perubahan yang didefinisikan, dan pengelolaan terhadap pelaksanaan proses secara efektif dalam mendukung terlaksananya pencapaian tujuan untuk peningkatan proses.



Gambar 2.5
COBIT 5 *Process Capability Model* (ISACA, 2012:42)

Indikator penilaian, ditunjukkan pada gambar 2.5, digunakan untuk melakukan penilaian apakah atribut pada proses telah tercapai. Berikut ini ada 2 (dua) jenis indikator penilaian yaitu :

1. Indikator atribut *capability*, yang berlaku untuk level *capability level* 2 sampai 5.
2. Memproses indikator kinerja, yang berlaku khusus untuk *capability level* 1.

Selanjutnya setelah proses teridentifikasi pada *Capability Level*, dilakukan pengukuran dengan memberikan skala *rating* pada setiap atribut tiap level dengan menggunakan skala sebagai berikut :

1. *Not Achieved* (N) artinya ada bukti yang sedikit atau bukti yang tidak ada pada pencapaian atribut yang telah didefinisikan pada proses yang dilakukan penilaian.
2. *Partially Achieved* (P) artinya ada beberapa bukti pada pendekatan dan pencapaian pada atribut yang telah ditentukan pada proses yang telah dinilai kemudian dari beberapa aspek pada pencapaian atribut tersebut tidak bisa diprediksi.

3. *Largely Achieved* (L) artinya ada bukti pada pendekatan yang sistematis dan hasil pada pencapaian yang signifikan dari atribut yang telah didefinisikan dalam proses yang dinilai. Beberapa kelemahan terkait dengan atribut adalah ada pada proses yang dinilai.
4. *Fully Achieved* (F) artinya ada bukti yang lengkap dan pendekatan yang sistematis dan pencapaian secara penuh dari atribut yang telah ditentukan dalam proses yang dinilai. Tidak ada kelemahan secara signifikan terkait atribut ini pada proses yang akan dinilai. Persentasi tingkat *capability* dengan menggunakan *rating* pada tabel 2.1

Tabel 2.1 Persentase Skala *Rating*

Abbreviation	*Description*	*%Achieved*
N	*Not Achieved*	0% sampai 50%
P	*Partially Achieved*	>15% sampai 50%
L	*Largely Achieved*	>50% sampai 85%
F	*Fully Achieved*	>85% sampai 100%

2.3.6 Metode Perhitungan Guttman

Salah satu metode perhitungan untuk kuesioner adalah menggunakan skala Guttman. Skala Guttman adalah skala perhitungan yang digunakan untuk melakukan pengukuran dengan tipe jawaban yang bersifat tegas yaitu “ya” atau “tidak”, “benar” atau “salah”, dan lain-lain. Data yang diperoleh yaitu berupa data dengan skala interval atau rasio dikotomi (dua alternatif). (Triana, 2013:185)

Selanjutnya setelah data kuesioner terkumpul kemudian hasil isian kuesioner yang berdasarkan kepada *governance* atau *management practice* dan *output* yang dihasilkan berupa “Ya” bernilai 1 dan “Tidak” bernilai 0. Skala *Governance/Management Practice* dihitung dengan menggunakan rumus sebagai berikut :

$$\text{Skala } \textit{Governance/Management practice} = \frac{\text{Jumlah jawaban “Ya”}}{\text{Total “Ya” dan “Tidak”}} \times 100\%$$

Sedangkan rumus Skala *Workproduct* yaitu :

$$\text{Skala } \textit{Workproduct} = \frac{\text{Jumlah jawaban “Ya”}}{\text{Total “Ya” dan “Tidak”}} \times 100\%$$

2.4 COBIT 5 Domain DSS (*Deliver, Service, and Support*)

Domain DSS berfokus pada aspek pengiriman teknologi informasi (TI) yang mencakup pada bidang-bidang pelaksanaan sistem TI yang efektif dan efisien. Domain DSS ini terdiri dari 6 sub proses dan 38 sub-sub proses, serta 204 aktivitas yang dilakukan pada domain ini. (Andry, 2017:2)

2.4.1 DSS01 *Manage Operations*

Proses DSS01 (*Deliver, Service and Support*) merupakan proses COBIT 5 yang menyeleraskan dan melaksanakan kegiatan dan prosedur operasional yang diperlukan pada saat memberikan layanan TI internal dan *outsourcing*, termasuk pelaksanaan *standard operational procedure* (SOP) yang telah ditetapkan dan kegiatan pemantauan yang diperlukan. Tujuan proses ini adalah memberikan hasil operasional TI sesuai dengan rencana.

1. DSS01.01 *Perform operational procedures*

   Menjaga dan melakukan prosedur dan tugas operasional secara andal dan konsisten.

2. DSS01.02 *Manage outsourced IT service*

   Mengelola layanan operasional TI dari pihak ketiga untuk menjaga perlindungan informasi organisasi dan keandalan penyampaian layanan.

3. DSS01.03 *Monitor IT infrastructure*

   Melakukan pemantauan infrastruktur TI yang terkait dan menyimpan kronologis informasi yang cukup dalam *log (*rekaman*)* operasi.

4. DSS01.04 *Manage the environment*

   Tindakan pertahanan yang dilakukan untuk melakukan perlindungan terhadap faktor lingkungan. Memasang peralatan dan alat perangkat khusus yang digunakan untuk memantau dan mengendalikan lingkungan.

5. DSS01.05 *Manage facilities*

   Mengelola terkait fasilitas, termasuk peralatan listrik dan komunikasi, yang sesuai dengan peraturan perundang-undangan, persyaratan teknis dan bisnis, spesifikasi *vendor*.

2.4.2 DSS02 *Manage service requests and incidents*

Memberikan tanggapan yang efektif dan tepat waktu terhadap permintaan dari pengguna (*user*) dan resolusi semua insiden. Mengembalikan ke layanan menjadi normal, merekam dan memenuhi permintaan pengguna, dan merekam, menyelidiki, mendiagnosis, meningkatkan dan menyelesaikan insiden. Tujuannya untuk mencapai meningkatkan produktivitas dan meminimalkan gangguan melalui penyelesaian yang cepat dari pertanyaan pengguna (*user*) dan insiden.

1. DSS02.01 *Define incident and service request classification schemes*

   Menentukan skema dan model klasifikasi permintaan dan layanan.

2. DSS02.02 *Record, classify and prioritise requests and incidents*

   Mengidentifikasi, mencatat dan mengklasifikasikan permintaan dan insiden layanan, kemudian menetapkan berdasarkan skala prioritas mulai dari kekritisan dan kesepakatan layanan bisnis.

3. DSS02.03 *Verify, approve and fulfill service requests*

   Melakukan pemilihan prosedur permintaan yang sesuai dan memastikan bahwa permintaan layanan tersebut sesuai dengan kriteria yang telah ditentukan.

4. DSS02.04 *Investigate, diagnose and allocate incidents*

   Mengidentifikasi, mencatat gejala kejadian, kemudian menentukan penyebab yang memungkinkan, dan mengalokasikan resolusi.

5. DSS02.05 *Resolve and recover from incidents*

   Mendokumentasikan, menerapkan dan menguji terhadap solusi yang teridentifikasi dan melaksnkan tindakan pemulihan untuk memulihkan layanan terkait TI.

6. DSS02.06 *Close service requests and incidents*

   Melakukan verifikasi terhadap penyelesaian insiden yang memuaskan dan/atau pemenuhan terhadap permintaan, dan menutup permintaan.

7. DSS02.07 *Track status and produce reports*

   Secara teratur melacak, menganalisis dan melaporkan kejadian (*event*) dan meminta pemenuhan terhadap tren untuk memberikan informasi perbaikan secara terus menerus.

2.4.3 DSS03 *Manage problems*

Mengidentifikasi dan mengklasifikasikan masalah serta akar dari permasalahannya dan memberikan resolusi yang tepat waktu dalam mencegah kejadian yang akan terulang kembali dan memberikan rekomendasi untuk perbaikan. Tujuannya untuk meningkatkan ketersediaan, meningkatkan tingkat layanan, mengurangi biaya, dan meningkatkan kenyamanan dan kepuasan pelanggan dengan mengurangi jumlah masalah operasional.

1. DSS03.01 *Identify and classify problems*

   Menentukan dan menerapkan terkait kriteria dan prosedur untuk melaporkan masalah yang teridentifikasi, termasuk pada klasifikasi masalah, kategori masalah dan prioritas masalah.

2. DSS03.02 *Investigate and diagnose problems*

   Menyelidiki dan mendiagnosis terhadap masalah yang relevan untuk menilai dan menganalisis pada akar permasalahan.

3. DSS03.03 *Raise known errors*

   Setelah mengidentifikasi dan mengetahui akar penyebab masalah, kemudian membuat catatan kesalahan yang diketahui dan solusi yang sesuai, dan identifikasi solusi potensial.

4. DSS03.04 *Resolve and close problems*

   Melakukan identifikasi dan memulai solusi berkesinambungan yang menangani akar dari permasalahan, meningkatkan permintaan terhadap perubahan melalui proses manajemen perubahan yang stabil jika diperlukan untuk menyelesaikan kesalahan. Memastikan personil yang terkena dampak, sadar terhadap tindakan yang akan diambil dan rencana yang akan dikembangkan dalam mencegah kejadian dimasa depan terjadi.

5. DSS03.05 *Perform proactive problem management*

   Menghimpun dan menganalisis data operasional (terutama catatan kejadian dan catatan perubahan) untuk mengidentifikasi terhadap kecenderungan yang muncul

dan mungkin mengindikasi masalah. *Log* catatan masalah untuk mengaktifkan penilaian.

2.4.4 DSS04 *Manage continuity*

Menetapkan dan memelihara terkait rencana untuk memungkinkan bisnis dan TI menanggapi insiden dan gangguan, agar dapat melanjutkan ke proses bisnis yang sangat penting dan memerlukan layanan TI dan menjaga atas ketersediaan informasi pada tingkat yang dapat diterima oleh organisasi. Tujuannya adalah untuk melanjutkan operasional bisnis yang sifatnya penting dan mempertahankan ketersediaan atas informasi pada tingkat layanan yang dapat diterima oleh organisasi.

1. DSS04.01 *Define the business continuity policy, objectives and scope*

   Menentukan kebijakan dan cakupan yang berkesinambungan sejalan dengan usaha dan tujuan organisasi dan pemangku kepentingan.

2. DSS04.02 *Maintain a continuity strategy*

   Memilih evaluasi manajemen kontinuitas bisnis dan memilih strategi kontinuitas berkelanjutan hemat biaya yang akan memastikan pemulihan dan kontinuitas organisasi dalam menghadapi bencana atau kejadian besar atau gangguan lainnya.

3. DSS04.03 *Develop and implement a business continuity response*

   Mengembangkan rencana bisnis berkelanjutan (BCP) berdasarkan strategi yang mendokumentasikan prosedur dan informasi untuk digunakan dalam suatu kejadian agar organisasi dapat melanjutkan kegiatan kritisnya.

4. DSS04.04 *Exercise, test and review the BCP*

   Melakukan uji pengaturan kontinuitas secara teratur untuk melaksanakan rencana pemulihan terhadap hasil yang telah ditentukan dan untuk memungkinkan solusi inovatif yang dikembangkan untuk membantu memverifikasi dari waktu sampai waktu selanjutnya bahwa rencana tersebut akan berjalan seperti yang diantisipasi.

5. DSS04.05 *Review, maintain and improve the continuity plan training*

   Melakukan tinjauan manajemen terhadap kemampuan kontinuitas secara berkala untuk memastikan kesesuaian, kecukupan dan efektivitas yang berkesinambungan. Mengelola perubahan rencana sesuai dengan proses pengendalian perubahan

untuk memastikan bahwa rencana kontinuitas tetap terjaga dan terus mencerminkan persyaratan bisnis yang sebenarnya.

6. DSS04.06 *Conduct continuity plan training*

   Memberikan kepada semua pihak internal dan eksternal yang bersangkutan dengan sesi pelatihan reguler mengenai prosedur dan tanggung jawab jika terjadi gangguan.

7. DSS04.07 *Manage backup arrangement*

   Mempertahankan ketersediaan informasi bisnis yang penting.

8. DSS04.08 *Conduct post-resumption review*

   Menilai kecukupan BCP setelah dimulainya kembali proses bisnis dan layanan setelah terjadi gangguan.

2.4.5 DSS05 *Manage security services*

Melindungi informasi pada organisasi dengan tujuan menjaga tingkat risiko pada keamanan informasi yang dapat diterima oleh organisasi sesuai dengan kebijakan keamanan. Menetapkan dan memelihara peranan terhadap keamanan informasi, hak akses dan melakukan pemantauan keamanan.

1. DSS05.01 *Protect against malware*

   Melaksanaan dan memelihara tindakan pencegahan, detektif dan melakukan perbaikan yang ada (terutama *patch* keamanan dan pengendalian virus yang terkini) di seluruh organisasi untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (misalnya *virus, worm, spyware, spam*).

2. DSS05.02 *Manage network and connectivity security*

   Menggunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi infromasi dari semua metode konektivitas.

3. DSS05.03 *Manage endpoint security*

   Memastikan titik akhir (*endpoint*) yang dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang telah ditetapkan.

4. DSS05.04 *Manage user identity and logical access*

   Memastikan semua pengguna (*user*) yang memiliki hak akses terhadap informasi

sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola akses mereka sendiri dalam proses bisnis.

5. DSS05.05 *Manage physical access to IT assets*

   Menentukan dan menerapkan prosedur untuk memberi, membatasi, dan mencabut akses masuk ke bangunan dan area yang sesuai dengan kebutuhan bisnis, termasuk saat terjadi keadaan darurat. Akses bangunan dan area harus dibenarkan, disahkan, dicatat, dan dipantau. Hal ini berlaku untuk semua orang yang akan memasuki tempat itu, termasuk staf, staf sementara, klien, *vendor*, pengunjung dan pihak ketiga lainnya.

6. DSS05.06 *Manage sensitive documents and output devices*

   Menetapkan pengamanan secara fisik, praktik akuntansi dan pengelolaan terhadap persediaan yang tepat atas aset TI yang sifatnya sensitif.

7. DSS05.07 *Monitor the infrastructure for security-related events*

   Menggunakan alat deteksi instrusi, memantau infrastruktur untuk akses dan memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian secara umum.

2.4.6 DSS06 *Manage business process*

Menentukan dan mempertahankan pengendalian proses bisnis secara tepat untuk memastikan bahwa informasi yang saling berkaitan akan diproses oleh proses bisnis *in-house* atau *outsourced* memenuhi terhadap semua persyaratan pengendalian informasi yang relevan. Mengidentifikasi persyaratan terhadap pengendalian informasi yang relevan, mengelola mengoperasikan terhadap pengendalian yang memadai untuk memastikan bahwa pemrosesan informasi yang memenuhi persyaratan. Tujuannya adalah untuk menjaga integritas informasi dan keamanan aset informasi yang ditangani dalam proses bisnis di organisasi atau luar organisasi.

1. DSS06.01 *Align control activity embedded in business processes with enterprise objectives*

   Menilai dan memantau terus pelaksanaan kegiatan proses bisnis dan pengendalian

yang terkait, berdasarkan risiko dari organisasi, dan memastikan bahwa pengendalian pemrosesan selaras dengan kebutuhan bisnis.

2. DSS06.02 *Control the processing of information*

   Mengoperasikan pelaksanaan kegiatan proses bisnis dan pengendalian yang terkait, berdasarkan risiko organisasi, untuk memastikan agar pemrosesan informasi benar, lengkap, tepat waktu, akurat dan aman.

3. DSS06.03 *Manage roles, responsibilities, access privillages and level authority*

   Menengelola peran bisnis, tanggung jawab, dan tingkat kewenangan dan segregasi tugas yang dibutuhkan untuk menunjang tujuan proses bisnis. Otorisasi akses terhadap aset informasi yang terkait dengan proses informasi bisnis, termasuk yang berada dibawah pengawasan bisnis, TI dan pihak ketiga. Bahwa ini memastikan bahwa bisnis telah mengetahui dimana keberadaan data dan siapa yang menangani data atas namanya.

4. DSS06.04 *Manage error and exceptions*

   Mengelola pengecualian pada proses bisnis, kesalahan dan memudahkan koreksi mereka. Menyertakn eskalasi kesalahan dan pengecualian proses bisnis dan melakukan eksekusi tindakan perbaikan yang ditentukan. Ini akan memberikan kepastian keakuratan dan integritas proses informasi bisnis.

5. DSS06.05 *Ensure traceability of informations events and accountabilities*

   Memastikan informasi bisnis dapat dilacak ke acara bisnis yang berasal dan pihak yang bertanggung jawab. Hal ini memungkinkan penelusuran informasi melalui siklus hidup dan proses terkaitnya. Ini memberikan kepastian bahwa informasi yang mendorong bisnis tersebut dapat diandalkan dan telah diproses sesuai dengan tujuan yang ditetapkan.

6. DSS06.06 *Secure information assets*

   Mengamankan terkait aset informasi yang hanya dapat diakses oleh bisnis melalui metode yang disetujui, termasuk informasi dalam bentuk elektronik, bentuk fisik, dan informasi selama transit. Ini menguntungkan bisnis dengan menyediakan perlindungan informasi dari ujung ke ujung.

2.5 RACI *Chart*

RACI merupakan singkatan dari *Responsible, Accountable, Consluted and Informed* (Setiaji, 3-4) adalah bagian kecil dari manajemen sumber daya manusia. RACI *Chart* sebagai alat yang dapat digunakan pada proses pengambilan keputusan dan akan membantu pada pihak manajemen saat mengidentifikasi peran serta tanggung jawab pegawai pada organisasi. Pembagian tugas secara jelas serta peran dan tanggung jawab merupakan hal yang sangat penting dalam suatu organisasi. Ketidakjelasan peran serta tanggung jawab akan menyebabkan kebingungan yang akhirnya dapat mengakibatkan berkurangnya produktivitas kerja pegawainya. RACI *Chart* terdiri 4 (empat) parameter utama, berupa :

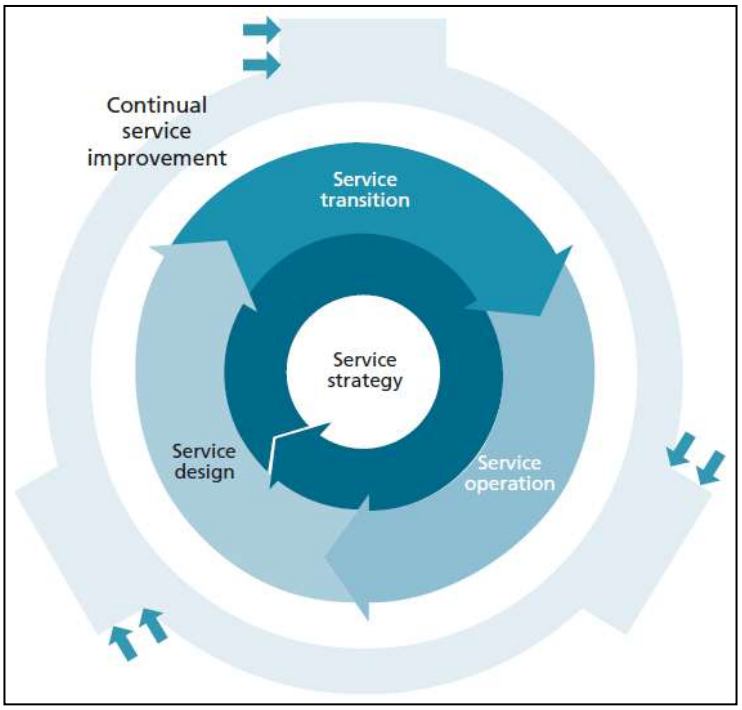
1. *Responsible*, yaitu orang yang melaksanakan tugas atau pekerjaan.
2. *Accountable*, yaitu orang yang bertanggung jawab terhadap suatu tugas atau pekerjaan serta memiliki wewenang terhadap pengambilan keputusan dari suatu permasalahan.
3. *Consulted*, yaitu orang yang memberikan saran, masukan, pendapat atau kontribusi ketika diperlukan saat melaksanakan tugas.
4. *Informed*, yaitu orang yang perlu mengetahui terhadap tindakan dan hasil suatu keputusan yang telah diambil.

2.6 ITIL (*Information Technology Infrastructure Library*) V3

ITIL adalah bagian dari serangkaian publikasi *best practices* pada *IT Service Management* (ITSM) atau manajemen layanan TI. (ITSMF, 2011:3) ITIL menyediakan pedoman untuk penyedia layanan mengenai kualitas layanan TI, proses, fungsi dan kemampuan lain yang diperlukan untuk mendukungnya. ITIL telah banyak digunakan berbagai organisasi atau perusahaan yang menyediakan layanan di seluruh dunia. ITIL bukan panduan yang harus diikuti, tetapi itu adalah pedoman atau standar yang harus dibaca dan dipahami, dan digunakan untuk menciptakan nilai bagi penyedia layanan dan pelanggannya. Organisasi didorong untuk mengadopsi *best practice* pada ITIL yang menyesuaikan pada lingkungan yang spesifik di organisasi dengan cara yang memenuhi kebutuhan oragnisasi tersebut.

ITIL adalah kerangka kerja yang paling dikenal luas untuk ITSM secara global diseluruh dunia. Pada 20 tahun terakhir sejak diciptakannya, ITIL telah melakukan revolusi dan mengubah luas seiring dengan perkembangan teknologi dan praktik bisnis. ISO / IEC 20000 memberikan standar formal dan universal untuk organisasi agar kemampuan manajemen layanannya diaudit dan disertifikasi. Sementara ISO/IEC 20000 adalah standar yang mesti dicapai dan dipertahankan, maka solusinya adalah ITIL menawarkan pengetahuan yang berguna untuk mencapai standar tersebut.

Selain publikasi inti, ada juga satu set publikasi ITIL yang saling melengkapi yang memberikan panduan pada sektor industri, jenis-jenis organisasi, model operasi, dan arsitektur teknologi.



Gambar 2.6
ITIL Lifecycle (ITSMF, 2011:3)

2.6.1 ITIL V3 2011

Seperti yang tertuang pada gambar 2.6 diatas, inti ITIL terdiri dari lima tahap publikasi *lifecycle*. Masing-masing memberikan panduan yang diperlukan untuk pendekatan terpadu seperti yang disyaratkan oleh spesifikasi standar ISO/IEC 20000. Kelima tahap publikasi *ITIL Lifecycle* (ITSMF, 2011:5-7) tersebut adalah :

1. ITIL *Service Strategy*

   Pada inti *ITIL lifecycle* terdapat *service strategy*. Penciptaan nilai ini dimulai di *service strategy* yaitu dengan memahami tujuan organisasi dan kebutuhan pelanggan. Setiap aset yang ada pada organisasi yaitu orang, proses dan produk harus mendukung strategi.

   ITIL *service strategy* berupa panduan mengenai manajemen layanan yang dilihat bukan dari kemampuan organisasi tetapi sebagai aset strategis. Ini menggambarkan prinsip-prinsip yang mendasari praktik manajemen layanan yang berguna untuk mengembangkan kebijakan, panduan, dan proses manajemen layanan di seluruh ITIL *service lifecycle*.

   Pada ITIL *service strategy* meliputi pengembangan ruang pasar, karakteristik jenis penyedia layanan internal dan eksternal, layanan aset, portofolio layanan dan implementasi strategi melalui *service lifecycle*. Organisasi menggunakan ITIL *service strategy* untuk menetapkan tujuan dan harapan kinerja menuju melayani pelanggan dan pangsa pasar, untuk mengidentifikasi, memilih dan memprioritaskan peluang.

2. ITIL *Service Design*

   Layanan dapat memberikan nilai terhadap bisnis jika layanan harus dirancang dengan mempertimbangkan tujuan bisnis. Desain mencakup seluruh organisasi TI, oleh karena itu adalah organisasi secara keseluruhan yang memberikan dan mendukung layanan. *Service design* adalah tahap dalam *lifecycle* yang mengubah *service strategy* menjadi tujuan bisnis.

   ITIL *service design* memberikan panduan untuk mendesain dan mengembangkan layanan dan manajemen praktik layanan. Mencakup prinsip-prinsip desain dan metode untuk mengubah tujuan strategis menjadi portofolio layanan dan aset dari layanan. Ruang lingkup ITIL *service design* tidak hanya terbatas dan terpaku pada layanan baru tetapi termasuk perubahan dan perbaikan sangat diperlukan dalam meningkatkan atau mempertahankan nilai terhadap pelanggan selama siklus layanan, layanan kontinuitas, pencapaian pada tingkat layanan, dan kesesuaian

dengan pedoman dan peraturan. *Service design* memandu organisasi bagaimana cara mengembangkan kemampuan rancangan dalam manajemen layanan.

3. ITIL *Service Transition*

ITIL *Service Transition* memberikan panduan untuk pengembangan dan peningkatan kemampuan untuk memperkenalkan layanan baru dan yang diubah ke lingkungan yang didukung. Menjelaskan bagaimana caranya mentransisikan suatu organisasi dari suatu negara ke negara yang lainnya sambil mengendalikan risiko dan dukungan pengetahuan organisasi untuk mendukung keputusan. Dan memastikan bahwa nilai diidentifikasi dalam *service strategy*, dan ditunjukkan dalam *service design*, secara efektif yang ditransisikan sehingga mereka dapat direalisasikan dalam *service operation*.

ITIL *Service Transition* merupakan *best practice* pada perencanaan dan dukungan transisi, manajemen perubahan, aset dan konfigurasi layanan manajemen, rilis dan manajemen penyebaran, layanan validasi dan pengujian, evaluasi perubahan dan manajemen pengetahuan. Ini memberikan panduan tentang mengelola kompleksitas yang terkait dengan perubahan layanan dan proses manajemen layanan, mencegah konsekuensi yang tidak diinginkan sambil memungkinkan untuk melakukan inovasi.

ITIL *Service Transition* juga memperkenalkan sistem manajemen pengetahuan layanan, yang dapat mendukung pembelajaran organisasi dan membantu meningkatkan efisiensi dan efektivitas secara keseluruhan dari semua tahap *service lifecycle*. Ini akan memungkinkan orang akan mendapatkan manfaat dari pengetahuan dan pengalaman orang lain, mendukung pengambilan keputusan berdasarkan informasi, dan meningkatkan manajemen layanan.

4. ITIL *Service Operation*

ITIL *Service Operation* menjelaskan *best practice* untuk mengelola layanan di lingkungan yang didukung. Ini termasuk panduan untuk mencapai efektivitas dan efisiensi pada pengiriman dan dukungan layanan yang memastikan terhadap nilai bagi pelanggan, pengguna dan penyedia layanan.

Tujuan strategis diwujudkan melalui layanan operasional oleh karena itu kemampuan menjadikannya sangat penting. ITIL *Service Operation* memberikan panduan tentang cara menjaga stabilitas, dalam *service operation* memungkinkan terhadap pelaksanan perubahan dalam desain, skala, ruang lingkup dan tingkat layanan. Organisasi akan menyediakan pedoman proses yang terperinci, dengan menggunakan metode dan alat dalam dua perspektif kontrol utama yaitu reaktif dan proaktif. Manajer dan praktisi diberikan pengetahuan yang memungkinkan mereka untuk membuat suatu keputusan yang lebih baik pada pengelolaan ketersediaan layanan, pengendalian permintaan, pengoptimalan pemanfaatan kapasitas, penjadwalan operasi, dan menghindari atau menyelesaikan insiden layanan dan mengelola masalah.

Pada ITIL *Service Operation* didalamnya terdapat pengelolaan *event management, incident management, request fulfilment, problem management* dan akses proses manajemen; serta meja layanan (*service desk*), manajemen teknis, manajemen operasional TI dan fungsi manajemen aplikasi.

5. ITIL *Continual Service Improvement*

ITIL *Continual Service Improvement* menyediakan panduan untuk menciptakan dan mempertahankan nilai untuk pelanggan melalui strategi, desain, transisi dan pengoperasian layanan. Ini menggabungkan prinsip, praktik, dan metode manajemen kualitas, manajemen perubahan dan kemampuan perbaikan.

ITIL *Continual Service Improvement* menggambarkan *best practice* untuk mencapai peningkatan yang bertahap dan skala besar dalam hal kualitas layanan, efisiensi operasional dan kontinuitas bisnis, dan untuk memastikan bahwa portofolio layanan terus diselaraskan dengan kebutuhan bisnis. Panduan diberikan untuk menghubungkan upaya dan hasil perbaikan dengan strategi layanan, desain, transisi dan operasi. Sistem loop umpan balik tertutup, berdasarkan *Plan-Do-Check*- Siklus UU (PDCA) yang dibentuk. Dimana umpan balik dari setiap tahapan siklus layanan agar dapat digunakan untuk mengidentifikasi terhadap peluang peningkatan untuk setiap tahap lain dari siklus hidup.

ITIL *Continual Service Improvement* menangani pengukuran layanan, menunjukkan nilai dengan metrik, mengembangkan *baseline* dan penilaian jatuh tempo. Masing-masing membahas kemampuan yang berdampak langsung pada kinerja penyedia layanan. Intinya adalah diharapkan memberikan struktur, stabilitas dan kekuatan untuk kemampuan manajemen layanan, dengan prinsip, metode, dan alat yang tahan lama. Ini berfungsi agar melindungi investasi dan melakukan pengukuran, pembelajaran dan peningkatan. Panduan ITIL *service lifecycle*, memberikan tinjauan umum tentang tahapan siklus hidup yang dijelaskan dalam inti ITIL.

2.6.1 ITIL *Service Design*

Service design merupakan salah satu layanan pada ITIL *service lifecycle* setelah *service strategy*.

2.6.1.1 Tujuan *Service Design*

Tujuan dari *service design* (ITSMF, 2012:21) adalah untuk memastikan bahwa layanan yang baru atau yang diubah dan dirancang untuk memenuhi persyaratan perubahan bisnis. *Service design* adalah salah satu tahap pada ITIL *lifecycle* yang mengubah persyaratan yang semula strategi layanan menjadi desain dengan tujuan untuk mewujudkan tujuan bisnis.

Kegiatan utama dalam tahap siklus hidup ini termasuk perencanaan dan koordinasi kegiatan desain, memastikan layanan desain yang konsisten, sistem informasi manajemen layanan, arsitektur, teknologi, proses, informasi dan metrik, produksi paket desain layanan (SDP), manajemen antarmuka, dan peningkatan kegiatan dan proses desain layanan.

ITIL *Service Design* menyediakan :

1. Panduan untuk desain dan pengembangan pada layanan dan praktik manajemen layanan.
2. Prinsip desain dan metode untuk mengubah tujuan strategis menjadi portofolio layanan dan aset layanan.

2.6.1.2 Proses dan kegiatan utama *Service Design*

1. *IT service continuity management*

Saat ini teknologi adalah komponen utama dari sebagian besar proses bisnis, ketersediaan TI yang tinggi yang terus menerus berperan penting untuk siklus hidup bisnis secara keseluruhan. Ini dicapai dengan memperkenalkan langkah-langkah dari pengurangan risiko dan pilihan pemulihan. Pemeliharaan kemampuan pemulihan yang berkelanjutan sangat penting jika ingin tetap efektif.

Tujuan dari *IT service continuity management* (ITSCM) adalah untuk mempertahankan kemampuan pemulihan berkelanjutan yang sesuai dalam layanan TI agar sesuai dengan kebutuhan, persyaratan, dan rentang waktu bisnis yang telah disepakati.

ITSCM mencakup serangkaian kegiatan di sepanjang siklus hidup untuk memastikan kesinambungan layanan dan rencana pemulihan telah dikembangkan, dan tetap selaras dengan rencana bisnis yang kesinambungan dan prioritas bisnis.

2. *Information security management*

Manajemen keamanan informasi (ISM) perlu dipertimbangkan dalam kerangka tata kelola orgnisasi secara keseluruhan. Tata kelola organisasi adalah serangkaian tanggung jawab dan praktik yang dilakukan oleh dewan dan manajemen eksekutif dengan empat tujuan memberikan arahan strategis, memastikan bahwa tujuannya telah tercapai, memastikan bahwa risiko dikelola dengan tepat, dan memverifikasi bahwa sumber daya organisasi digunakan secara efektif.

Tujuan dari proses ISM adalah untuk menyelaraskan antara keamanan TI dengan keamanan bisnis dan memastikan bahwa keamanan informasi telah dikelola secara efektif dalam semua kegiatan manajemen layanan, yaitu :

a. *Availability* yaitu informasi tersedia dan dapat digunakan bila diperlukan.
b. *Confidentiality* Informasi diamati oleh atau diungkapkan hanya kepada yang memiliki hak akses.
c. *Integrity* informasi lengkap, akurat, dan terlindungi dari modifikasi orang yang tidak sah.

d. *Authenticity and non-repudiation* Transaksi bisnis, serta pertukaran informasi, dapat dipercaya ISM mempertahankan dan menegakkan kebijakan secara keseluruhan, bersama dengan serangkaian pengendlian pendukung dalam manajemen keamanan terpadu sistem informasi, selaras dengan kebijakan dan strategi keamanan bisnis.

2.6.2 ITIL *Service Operation*

Service Operation merupakan salah satu layanan publikasi *lifecycle* pada ITIL V3 2011 setelah *service transition* yang didalamnya terdapat tujuan dan proses dan kegiatan utama layanan TI.

2.6.2.1 Tujuan *Service Operation*

Tujuan dari *Service Operation* (ITSMF, 2012:40) adalah untuk memberikan tingkat layanan yang disepakati kepada pengguna dan pelanggan, untuk mengelola aplikasi, teknologi, dan infrastruktur yang mendukung pada pengiriman layanan. *Service Operation* juga merupakan satu-satunya fase dalam *service lifecycle* yang memiliki fungsi yang ditentukan di dalamnya. Ada empat fungsi seperti: *service desk*, *technical management*, *application management* dan *IT operation management*. Sementara fungsi-fungsi ini secara aktif mendukung fase lain dari l*ifecycle*, mereka berada dalam *service operation*.

Sebagai bagian dari *service lifecycle*, *service operation* bertanggung jawab untuk :

1. Menjalankan dan melakukan proses yang mengoptimalkan biaya dan kualitas layanan.
2. Memungkinkan bisnis untuk memenuhi tujuannya.

Sebagai bagian dari dunia teknologi, *service operation* bertanggung jawab atas :

1. Berfungsinya komponen yang efektif yang mendukung layanan.
2. Eksekusi kegiatan pengendalian operasi untuk mengelola dan memberikan layanan.

Sebagai bagian dari bisnis secara keseluruhan, *service operation* bertanggung jawab untuk :

1. Memberikan layanan secara efisien dan biaya yang dapat diterima.
2. Memberikan layanan dalam level layanan yang ditentukan.

3. Mempertahankan kepuasan pengguna dengan layanan TI.

2.6.2.2 Proses dan kegiatan utama *Service Operation*

1. *Event Management*

   Layanan operasional yang efektif dan tergantung pada status infrastruktur dan komponen di dalamnya. Jika suatu *event* dapat menunjukkan bahwa ada sesuatu yang berfungsi salah, berpotensi mengarah pada log kejadian yang diketahui. *Event* juga dapat menunjukkan bahwa kegiatan normal, atau intervensi rutin telah terjadi. Tujuan *event management* adalah untuk mengelola *event* sepanjang siklus hidupnya mulai dari mendeteksi sampai menentukan tindakan pengendalian yang sesuai.

   Pemantauan dan *event management* sangat erat kaitannya tetapi sifatnya berbeda sedikit. *Event management* berfokus pada proses mendeteksi dan memberitahukan tentang status infrastruktur dan layanan TI. Pemantauan hanya mengawasi infrastruktur dan layanan TI, melaporkan statusnya apakah berarti atau tidak.

2. *Incident Management*

   Insiden adalah gangguan yang tidak terencana pada layanan TI, atau penurunan kualitas layanan TI. Kegagalan terkait *item* konfigurasi yang belum mempengaruhi terhdap layanan juga merupakan insiden. Tujuan dari *incident management* adalah mengembalikan layanan menjadi kembali normal dengan cepat dan untuk meminimalkan dampak buruk pada operasi bisnis. Layanan ‘Normal’ adalah tingkat layanan yang disepakati dan ditentukan dalam SLA dan OLA.

   Insiden sering terdeteksi oleh *event management*, atau oleh pengguna yang menghubungi *service desk*. Insiden dikategorikan untuk mengidentifikasi siapa yang harus mengerjakannya dan untuk melakukan analisis berdasarkan tren, dan dilaksanakan berdasarkan skala prioritas sesuai dengan urgensi dan dampak terhadap bisnis.

3. *Request Fulfilment*

   Permintaan layanan adalah permintaan formal dari pengguna untuk sesuatu yang akan disediakan. Tujuan dari *request fulfilment* adalah untuk memungkinkan pengguna untuk meminta dan menerima standar layanan, untuk mencari dan

memberikan layanan ini, memberikan informasi kepada pengguna dan pelanggan tentang layanan, dan untuk membantu dengan informasi umum, keluhan, dan komentar. Skala dan risiko yang bersifat rendah yang sering membutuhkan proses yang terpisah ini daripada berpotensi mengalami insiden normal dan mengubah proses manajemen. Semua permintaan dicatat dan dilacak, biasanya melalui *service desk*, dan mungkin memerlukan tingkat otorisasi yang sesuai sebelum pemenuhan

4. *Problem Management*

   Tujuan dari *problem management* adalah untuk mengelola siklus hidup semua masalah, dari identifikasi pertama hingga investigasi dan dokumentasi untuk akhirnya dilakukan penghapusan. *Problem management* berusaha untuk meminimalkan dampak buruk dari insiden dan masalah yang secara proaktif mencegah terulangnya kembali insiden tersebut. Intinya adalah adalah tentang mencari akar penyebab insiden dan masalah dan memulai tindakan untuk memperbaiki atau memperbaiki situasi.

5. *Access Management*

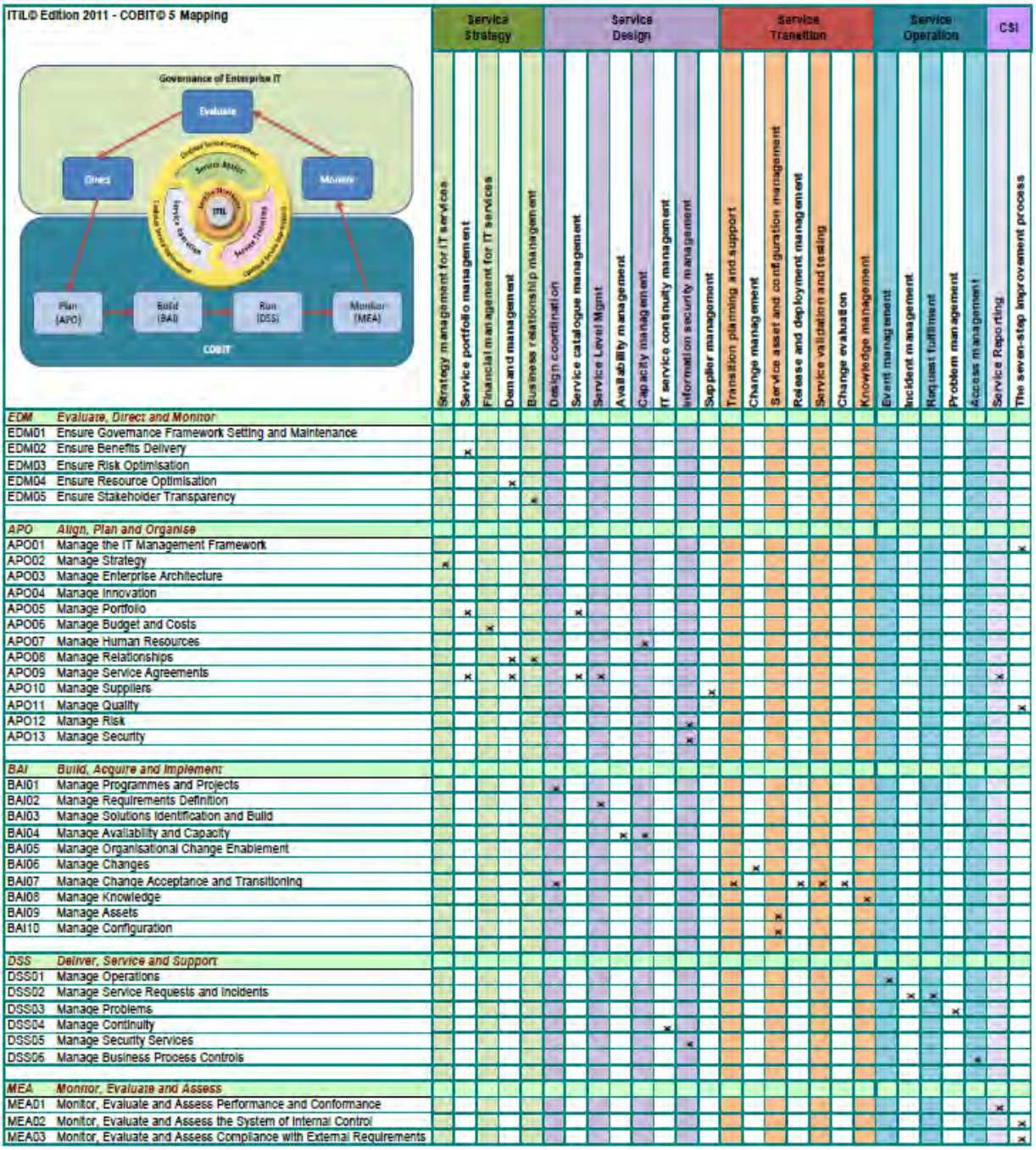
   Tujuan dari proses *access management* adalah untuk memberikan hak bagi pengguna untuk dapat mengakses layanan atau kelompok layanan, sambil mencegah akses ke pengguna yang tidak resmi. *Acess management* membantu mengelola kerahasiaan, ketersediaan, dan integritas data dan kekayaan intelektual. Ini adalah proses *userfacing* yang mendukung manajemen keamanan informasi.

2.7 Pemetaan COBIT 5 dan ITIL V3 2011

Perbedaan mendasar pada kerangka kerja ITIL adalah bagaimana proses-proses dijelaskan dan ditangani pada setiap aktivitas dan *flowchart* yang berbeda yang nantinya diharapkan akan memberikan sebuah arahan pada organisasi dalam penggunaan TI dengan efektif dan efisien. Sedangkan dari sisi *Critical Success Factor*, COBIT menjelaskan dengan secara lebih rinci dan lebih tepat sasaran.

COBIT memiliki struktur yang lebih baik dalam hal mengklasifikasikan masalah-masalah yang terkait dengan *IT Auditing*, dalam hal *IT Auditing* pada COBIT mencakup area yang lebih luas dan lebih cocok digunakan untuk menilai dan mengevaluasi sebuah

IT Governance. Fitur-fitur pada COBIT dalam penanganan terhadap masalah yang berkaitan dengan manajemen adalah COBIT mampu mereferensikan *Critical Success Factor* dengan indikator kinerja dan model kapabilitas *IT Governance*. (Simonsson dan Johnson, 2008) berargumen bahwa ITIL tidak mendukung minat dalam IT (*Strategic Interest of IT*). Dalam hal ini COBIT diakui memiliki struktur *IT Governance* yang lebih baik.



Gambar 2.7
Pemetaan COBIT 5 dan ITIL V3 2011

Pada gambar 2.9 diatas dapat terlihat antara COBIT dan ITIL, keduanya memiliki kesamaan dalam model dan struktur di bidang *IT Management*, terutama pada COBIT menggunakan kerangka kerja ITIL di versi terbaru keduanya. Ada beberapa masalah yang ditujukan oleh kerangka kerja ini dan terdapat sedikit perbedaan konotasi yang dapat dilihat dalam tabel berikut (Gehrmann, 2012).

Tabel 2.2 Pemetaan COBIT 5 dengan ITIL V3 2011

No	**COBIT 5**			**ITIL V3 2011**
	Area	**Domain**	**Process**	
1	*Governance*	*Evaluate, Direct, and Monitor*	EDM02 *Ensure Benefits Delivery*	SS *Service Protofolio Management*
			EDM04	SS *Demand Management*
			EDM05	SS *Business Relationship Management*
2	*Management*	*Align, Plan and Organise*	APO01 *Manage the IT Management Framework*	CSI *The seven step improvement process*
			APO02 *Manage Strategy*	SS *Strategy management for IT service*
			APO05 *Manage Portofolio*	SS *Service Portofolio Management*
				SD *Service Catalouge Management*
			APO06 *Manage Budget and Costs*	SS *Demand Management*
			APO07 *Manage Human Resources*	SS *Financial Management for IT service*
			APO08 *Manage Relationships*	SS *Demand Management*
				SS *Business Relationship Management*
			APO09 *Manage Service Agreement*	SS *Service Portofolio Management*
				SS *Demand Management*
				SD *Service Catalouge Management*
				SD *Service Level Management*
				CSI *Service Reporting*
			APO10 *Manage Suppliers*	SD *Supplier Management*
			APO11 *Manage Quality*	CSI *The seven step improvement process*
			APO12 *Manage Risk*	SO *Information Security Management*
			APO13 *Manage Security*	SO *Information Security Management*
		Build, Acquire and Implement	BAI01 *Manage Programmes and Projects*	SD *Design Coordination*
			BAI02 *Requirements Definition*	SD *Service Level Management*
			BAI04 *Manage Availability and Capacity*	SD *Availability Management*
				SD *Capacity Management*
			BAI06 *Manage Changes*	ST *Change Management*

No	COBIT 5			ITIL V3 2011
	Area	Domain	Process	
			BAI07 *Manage Change Acceptance and Transitioning*	SD *Design Coordination*
				ST *Transition Plannning and Support*
				ST *Release and Deploymemt Management*
				ST *Service Validation and Testing*
				ST *Change Evaluation*
			BAI08 *Knowledge*	ST *Knowledge Management*
			BAI09 *Assets*	ST *Service Asset and Configuration Management*
			BAI10 *Configuration*	ST *Service Asset and Configuration Management*
		Deliver, Service and Support	DSS01 *Manage operations*	SO *Event Management*
			DSS02 *Manage Service Request and Incidents*	SO *Incident Management*
				SO *Request Fulmfilment*
			DSS03 *Manage Problems*	SO *Problem Management*
			DSS04 *Manage Continuity*	SD *Service Coninuity Management*
			DSS05 *Manage Security Service*	SD *Service Security Management*
			DSS06 *Manage Business Process Controls*	SO *Acess Management*
		Monitor, Evaluate and Assess	MEA01 *Monitor, Evaluate and Assess Performance and Conformance*	CSI *Service Reporting*
			MEA02 *Monitor, Evaluate and Assess the System of Internal Control*	CSI *The seven step improvement process*
			MEA03 *Monitor, Evaluate and Assess Compliance with External Requirements*	CSI *The seven step improvement process*

Pada tabel diatas dijelaskan bahwa domain COBIT 5 berelasi dengan *service lifecycle* di ITIL V3 2011. Dalam Cobit 5 terdapat 2 (dua) area utama yaitu area *governance* (tata kelola) yaitu domain EDM (*Evaluate, Direct and Monitor*) sedangkan area *management* (manajemen) terdiri dari 3 (tiga) domain yaitu domain BAI (*Build, Acquire and Implement*), APO (*Align, Plan and Organise*), DSS (*Deliver, Service and Support*) dan MEA (*Monitor, Evaluate and Assess*). Sedangkan pada ITIL V3 2011 terdiri dari *Service Strategy, Service Design, Service Transition, Service Operation dan Continual Service Improvement.*

2.8 Kajian Pustaka

Ada beberapa penelitian yang menjadi acuan, seperti yang tertera pada tabel berikut ini :

Tabel 2.3 Daftar Penelitian tentang Audit/Evaluasi menggunakan COBIT 5 dan ITIL V3 2011

Nama	Judul Penelitian	Metode Penelitian	Kesimpulan	Lokasi
Faried Effendy, Bahana Sukma Dewa, dan Eva Hariyanti (2018). Jurnal Sistem Informasi Bisnis 02 (2018) On-line : http://ejournal.undip.ac.id/index.php/jsinbis. DOI : 10.21456/vol8iss2pp157-165	*Problem Management* Teknologi Informasi Berdasarkan Kerangka Kerja ITIL V3 2011 dan COBIT 5	1. Penyusunan SOP 2. Daftar Aktivitas ITIL V3 2011 *Problem Management* dan COBIT 5 DSS 03 3. Pemetaan Aktivitas ITIL V3 2011 *Problem Management* dan COBIT 5 DSS 03 4. Melakukan verifikasi aktivitas baru pada perusahaan 5. Pemetaan aktor aktivitas berdasarkan RACI DSS03 6. Pemetaan *workproduct* 7. Penyesuaian SOP 8. Wawancara untuk identifikasi kebutuhan 9. Pemetaan aktor aktivitas dengan struktur organisasi perusahaan 10. Verifikasi SOP 11. Mendatangi pihak manajemen apakah sudah sesuai atau tidak	Hasil akhir dari penelitian adalah penyusunan *Standar Operational Procedure* (SOP) dan hasil analisis daftar aktivitas-aktivitas *problem management* pada ITIL V3 2011 dan COBIT 5 pada domain DSS03 *Manage Problem*. Kemudian pemetaan ITIL V3 2011 pada *problem management* dan COBIT 5 pada domain DSS03 *Manage Problem*. Dokumen *Standar Operational Procedure* SOP *problem management* tersebut terdiri dari 11 prosedur dan 5 (lima) aktor. Kelima aktor tersebut mempunyai peranan yang akan melaksanakan *problem management* yaitu sebagai berikut: 15 aktivitas untuk *IT Support*, 15 aktifitas untuk *IT Manager*, 5 aktivitas untuk *IT Programmer*, 1 aktivitas untuk *General Manager*, dan 2 aktivitas untuk *IT* Dokumen.	Perusahaan Ekspor
Fachruddin Edi Nugroho Saputro, Ema Utami, dan	Integrasi Framework COBIT 5 dan ITIL V.3 Untuk Membangun Model	1. Studi Literatur, Mempelajari penelitian yang terdahulu dan buku-	Infrastruktur Teknologi Informasi mempunyai peranan yang penting bagi organisasi dan merupakan pondasi layanan teknologi informasi	-

Nama	Judul Penelitian	Metode Penelitian	Kesimpulan	Lokasi
Hanif Al Fatta (2018). Konferensi Nasional Sistem Informasi 2018, STMIK Atma Luhur Pangkalpinang, 8 – 9 Maret 2018	Tata Kelola Infrastruktur Teknologi Informasi	buku yang berhubungan dengan struktur organisasi, layanan teknologi informasi dan dokumen lain yang berhubungan dengan infrastruktur teknologi informasi. 2. Observasi, Observasi dilakukan dengan tujuan untuk mengetahui keadaan nyata proses bisnis yang berhubungan dengan infrastruktur teknologi informasi dan untuk mengetahui alur proses penggunaan infrastruktur teknologi informasi.	karena layanan teknologi informasi erat keterkaitannya dengan infrastruktur teknologi informasi. Pada tata kelola teknologi informasi, layanan teknologi informasi jika tidak dikelola secara baik maka akan menimbulkan biaya operasional yang tidak dapat diprediksi besarannya, layanan teknologi informasi tidak akan terkontrol dengan baik, dan pengambilan keputusan yang tidak akan tepat. Tata kelola teknologi informasi mempunyai kegunaan untuk menyelaraskan strategi TI dengan strategi bisnis pada organisasi. COBIT pada saat ini banyak digunakan untuk tata kelola teknologi informasi dan ITIL adalah kerangka kerja yang menggambarkan *best practice* dalam manajemen layanan TI. COBIT menjelaskan apa yang harus dilakukan dan ITIL menjelaskan secara rinci bagaimana melakukannya serta menyediakan panduan terhadap kegiatan apa yang harus dilakukan. Perpaduan antara COBIT dan ITIL dapat memperkuat tata kelola TI dengan kemungkinan yang lebih besar akan mendapat dukungan manajemen dan penggunaan TI yang lebih efektif dalam penerapan sumber daya pada tata kelola teknologi informasi. Integrasi COBIT 5 dan ITIL V3 2011 berdasarkan kepada *IT-Related Goals* pada COBIT 5. Penentuan domain COBIT 5 yang terkait dengan infrastruktur teknologi informasi berdasarkan pemetaan COBIT 5 *IT-Related Goals* dan COBIT 5 proses menggunakan skala primer. Hasil dari pemetaan didapatkan 5 domain yaitu EDM03, APO12, APO13, BAI06, dan DSS05 kemudian hasil dari pemetaan yang dapat diintegrasikan dengan ITIL V3 2011 ada 3 (tiga) domain yaitu APO13, BAI06, dan DSS05. Setelah mendapatkan 3 (tiga) domain hasil pemetaan	

Nama	Judul Penelitian	Metode Penelitian	Kesimpulan	Lokasi
			antara COBIT 5 dan ITIL V3 2011 maka selanjutnya adalah melakukan pengumpulan data dan kemudian menentukan responden berdasarkan diagram RACI pada COBIT 5. Hasil dari kuesioner di analisis dengan menggunakan PAM (*Process Assessment Model*) pada COBIT 5 dan rekomendasi perbaikan layanan berdasarkan kepada ITIL V3 2011 mengacu mapping dari COBIT 5. Rekomendasi perbaikan layanan disusun dalam bentuk matriks SWOT sehingga kemudian didapatkan strategi pada perbaikan layanan organisasi.	
Harfebi Fryonanda, Heru Sokoco, dan Yani Nurhadryani (2019). JUTI: Jurnal Ilmiah Teknologi Informasi - Volume 17, Nomor 1, Januari 2019: 1 – 11	Evaluasi Infrastruktur Teknologi Informasi dengan COBIT 5 dan ITIL V3 2011	1. Tata kelola Infrastruktur TI 2. Kepuasan Pengguna 3. Analisis SWOT	Kesimpulan yang didapat pada penelitian ini adalah mempelajari pengukuran tingkat kematangan TI dan pengukuran tingkat kepuasan pengguna terhadap layanan TI di IPB. Pada pengukuran tingkat kematangan TI menggunakan COBIT 5 dengan melakukan pengukuran 13 pro ses, dan pengukuran tingkat kepuasan pengguna dengan mengukur 11 (sebelas) kriteria dari 4 (empat) dimensi. Dari hasil pengukuran tingkat kematangan TI (saat ini) maka didapatkan 2 proses level 0, 8 proses level 1 dan 2 proses level 2. Dan tingkat harapan kematangan TI berada pada level 4 dan 5. Pada pengukuran tingkat kepuasan pengguna TI mendapat hasil 3 (tiga) kriteria di kuadran A, 2 kriteria di kuadran B, 2 kriteria di kuadran C dan 4 kriteria di kuadran D. Nilai harapan dapat dicapai yaitu dengan melakukan beberapa strategi perbaikan layanan TI. Hasil penelitian ini memberikan rekomendasi yang disusun dengan pendekatan model SWOT dan strategi perbaikan pada SWOT yang mengacu pada ITIL V3 2011 2011.	IPB

Nama	Judul Penelitian	Metode Penelitian	Kesimpulan	Lokasi
Aldi Satriani Wibowo, Selo, Dani Adipta (2016). Seminar Nasional Teknologi Informasi dan Komunikasi 2016 (SENTIKA 2016), Yogyakarta, 18-19 Maret 2016 (ISSN: 2089-9815)	Kombinasi Framework COBIT 5, ITIL dan ISO/IEC 27002 untuk membangun Model tata kelola teknologi informasi di Perguruan Tinggi	Kombinasi Antara COBIT, ITIL dan ISO/IEC 27002	Beberapa perusahaan menginginkan efisiensi penggunaan TI pada sesuai dengan tujuan strategis yang ingin dicapai oleh perusahaan. Efisiensi ini dapat dicapai melalui tata kelola teknologi informasi (*IT Governance*)yang cakupannya sangat luas dan kompleks. Tujuan dari *IT Governance* adalah untuk membantu organisasi meningkatkan keunggulan kompetitif perusahaan dengan pesaing. Keunggulan kompetitif pada perusahaan yang beroperasi secara efektif dan efisien. Efisiensi mempunyai arti menggunakan segala sesuai dengan efektif sedangkan efektivitas adalah mendapatkan nilai yang besar dengan hal yang benar. TI pada perusahaan harus dilakukan secara efisien yaitu meminimalkan risiko keamanan yang sesuai dengan persyaratan hukum. Usaha untuk mencapai hasil yang akan lebih baik dan memenuhi semua kebutuhan manajemen TI, maka dengan ini penulis ingin mengusulkan suatu kerangka kerja (*framework*) untuk tata kelola teknologi informasi yaitu ITIL, COBIT dan ISO/IEC 27002 untuk mencapai tujuan perusahaan. Kombinasi antara metodologi manajemen TI pada ITIL, COBIT dan ISO/IEC 27002 memberikan hasil pendekatan yang lebih komprehensif dan efisien. Selanjutnya akan memungkinkan fitur-fitur yang sebelumnya tidak dianggap pada penggunaan metode tunggal, maka akan mulai menjadi dapat diatasi dan dikendalikan oleh organisasi.	-
Ita Ernala Kaban	Tata Kelola Teknologi Informasi (*IT Governance*)	*IT Governance*	Kerangka kerja COBIT mempunyai kompromi antara dimensi horisontal dan dimensi vertikal yang lebih baik dari standar-standar lainnya. Pada COBIT mempunyai proses TI yang lebih luas dan lebih rinci. Selanjutnya kerangka kerja ITIL adalah standar yang paling rinci dan mendalam dalam	-

Nama	Judul Penelitian	Metode Penelitian	Kesimpulan	Lokasi
			mendefinisikan proses-proses TI yang sifatnya teknis dan operasional. Sedangkan pada Kerangka Kerja COSO detail yang dijelaskan dangkal, walaupun pada proses teknis dan operasional lebih luas. Penerapan TI memiliki risiko keamanan yang tinggi dan pengelolaan layanan TI yang tidak efisien akan menjadikan TI yang diterapkan akan menjadi *cost-center* perusahaan, malah bukan mencapai tujuan strategis perusahaan. Pada penelitian ini akan menganalisis potensi dan status pengelolaan TI di perusahaan, yang kemudian selanjutnya akan memberikan masukan agar investasi TI beserta pengelolaannya dengan standar internasional, dan menjadikannya *enabler* tercapainya sebagai tujuan organisasi yang tercantum dalam visi dan misi perusahaan.	

BAB III

OBJEK DAN METODOLOGI PENELITIAN

3.1 Profil Pengadilan Militer II-09 Bandung

Peradilan Militer adalah salah satu lembaga kekuasaan kehakiman di bawah Mahkamah Agung RI yang berfungsi menegakkan hukum yang independen, efektif, efisien dan berkeadilan khususnya di lingkungan Tentara Nasional Indonesia (TNI) dan bagi seluruh rakyat Indonesia pada umumnya. Sesuai Keputusan Presiden Republik Indonesia Nomor 56 Tahun 2004 tentang pengalihan organisasi, administrasi dan finansial pengadilan dalam lingkungan peradilan militer dari Markas Besar Tentara Nasional Indonesia ke Mahkamah Agung Republik Indonesia. Sejak bulan September 2015, Struktur Organisasi Peradilan Militer mengalami perubahan sesuai dengan Peraturan Mahkamah Agung R.I. Nomor 7 Tahun 2015 kemudian terbit Peraturan Mahkamah Agung RI Nomor 1 Tahun 2017 tanggal 17 Februari 2017 tentang Perubahan atas Peraturan Mahkamah Agung RI Nomor 7 Tahun 2015 tentang Organisasi dan Tata Kerja Kepaniteraan dan Kesekretariatan Peradilan tentang Organisasi dan Tata Kerja Kepaniteraan dan Kesekretariatan Peradilan sehingga sama dengan lingkungan peradilan lainnya.

Guna melaksanakan visi dan misinya sehingga terwujud badan peradilan yang ideal, Pengadilan Militer II-09 Bandung Tahun 2018 memiliki program Rencana Kerja Tahunan (RKT) meliputi pembinaan dan pengelolaan/manajemen organisasi serta pengawasan baik di bidang teknis yudisial maupun non teknis yudisial. Program kerja ini diwujudkan meliputi :

1. Melaksanakan fungsi kekuasaan kehakiman secara independen, efektif dan berkeadilan.
2. Didukung pengelolaan anggaran berbasis kinerja secara mandiri yang dialokasikan secara proporsional dalam APBN.
3. Memiliki struktur organisasi yang tepat dan manajemen organisasi yang jelas dan terukur.

4. Menyelenggarakan manajemen dan administrasi proses perkara yang sederhana, cepat, tepat waktu, biaya ringan dan proporsional.
5. Mengelola sarana prasarana dalam rangka mendukung lingkungan kerja yang aman, nyaman dan kondusif bagi penyelenggaraan peradilan.
6. Mengelola dan membina sumber daya manusia yang kompeten dengan kriteria obyektif, sehingga tercipta personil peradilan yang berintegritas dan profesional.
7. Didukung pengawasan secara efektif terhadap perilaku, administrasi, dan jalannya peradilan.
8. Berorientasi pada pelayanan publik yang prima.
9. Memiliki manajemen informasi yang menjamin akuntabilitas, kredibilitas, dan transparansi.
10. Modern dengan berbasis Teknologi Informasi terpadu.

Gambar 3.1
Peta Wilayah Hukum Pengadilan Militer II-09 Bandung di https://dilmil-bandung.go.id/sekilas-profil/

3.1.1 Visi dan Misi

1. Visi

   Visi adalah suatu gambaran tentang keadaan masa depan yang berisikan cita-cita dan citra yang ingin diwujudkan organisasi Pengadilan Militer II-09 Bandung. Visi berisi sebagai berikut : *"*Terwujudnya Pengadilan Militer II-09 Bandung yang agung*"*.

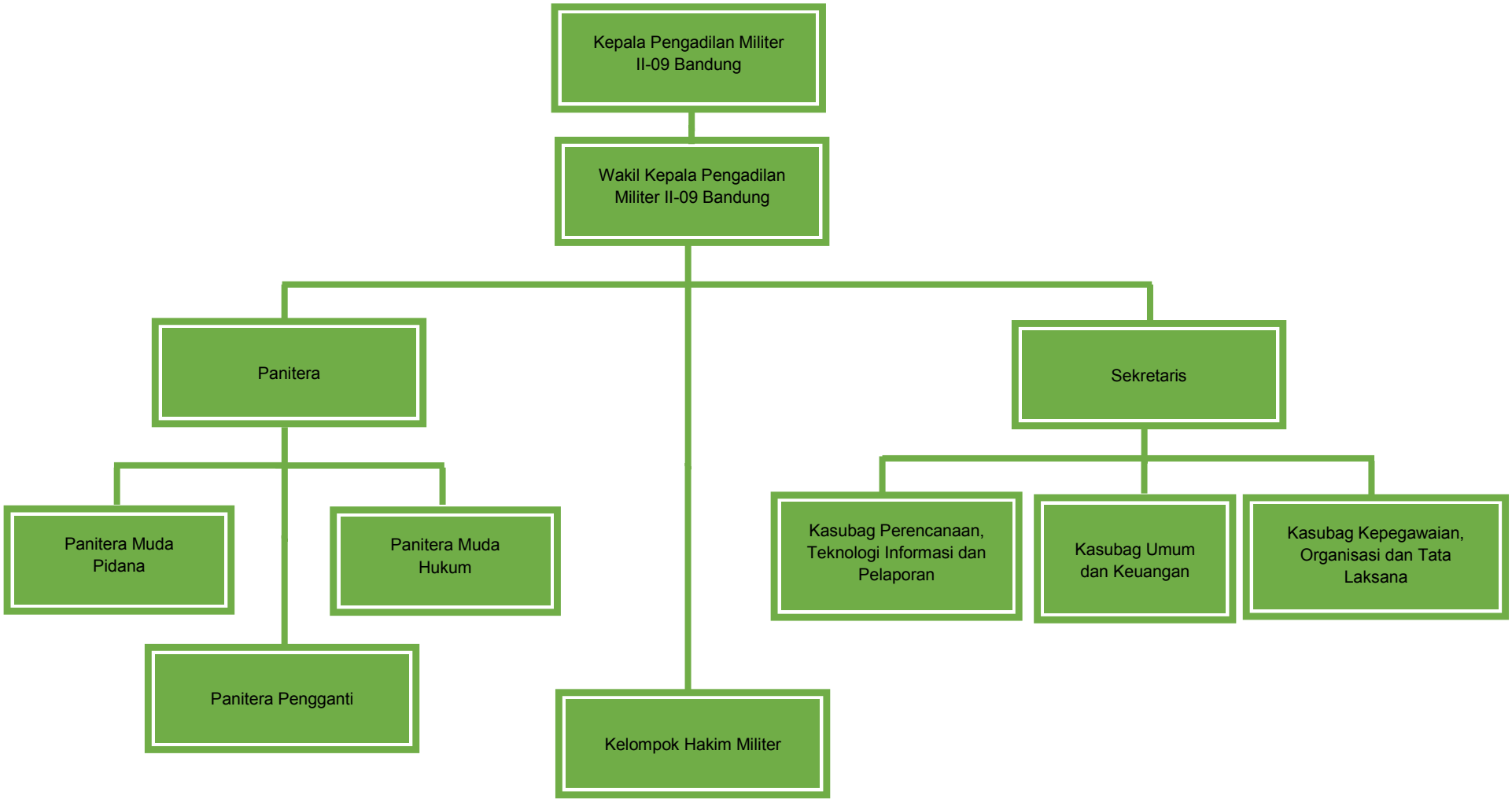
2. Misi

Visi tersebut akan dicapai melalui Misi yang dapat diuraikan sebagai berikut :

a. Menjaga kemandirian Pengadilan Militer II-09 Bandung.
b. Memberikan pelayanan hukum yang berkeadilan kepada pencari keadilan;
c. Meningkatkan kualitas kepemimpinan, profesionalisme tenaga teknis dan non teknis Pengadilan Militer II-09 Bandung
d. Meningkatkan kredibilitas dan transpransi Pengadilan Militer II-09 Bandung.

3.1.2 Struktur Organisasi

Struktur Organisasi pada Pengadilan Militer II-09 Bandung berdasarkan Peraturan Mahkamah Agung RI Nomor 7 Tahun 2015 tentang Organisasi dan Tata Kerja Kepaniteraan dan Kesekretariatan Peradilan adalah sebagai berikut :



Gambar 3.2
Struktur Organisasi Pengadilan Militer II-09 Bandung di https://dilmil-bandung.go.id/struktur-organisasi/

3.1.3 Tugas Pokok

Kesekretariatan terdiri dari 3 (tiga) sub bagian yang masing-masing dijabat oleh seorang Pama atau ASN Golongan III.B terdiri dari Sub Bagian Perencanaan, Teknoloogi Informasi dan Pelaporan, Sub Bagian Umum dan Keuangan, dan Sub Bagian Kepegawaian Organisasi dan Tata Laksana, sebagai berikut :

1. Sub Bagian Perencanaan, Teknologi Informasi dan Pelaporan.
    a. Perencanaan DIPA.
    b. Pengajuan Revisi DIPA dan POK.
    c. Pengelolaan Website.
    d. Pemeliharaan Sistem Informasi Penelusuran Perkara.
    e. Penyusunan Laporan.
2. Sub Bagian Umum dan Keuangan.
3. Sub Bagian Kepegawaian, Organisasi dan Tata Laksana.

3.1.4 Pemanfaatan Teknologi

Pada penerapan tata kelola teknologi informasi di Pengadilan Militer II-09 Bandung, diharapkan dapat memberikan peranan penting untuk pelaksanaan proses bisnis yaitu pelayanan publik bagi pelanggan internal maupun masyarakat pencari keadilan. Dengan dukungan teknologi informasi dengan layanan informasi yang cepat dan akurat disajikan kepada pelanggan dan pihak internal serta masyarkat.

Sesuai dengan maklumat pelayanan Pengadilan Militer II-09 Bandung terkait dengan peningkatan layanan yaitu pelayanan publik "*one day one publish*" akan mempublikasikan informasi perkara pada hari yang sama dengan perkara tersebut diputus.

Sebagai tindak lanjut dari Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan Nomor 25 Tahun 2009 tentang Pelayanan Publik, Surat Keputusan Ketua Mahkamah Agung Republik Indonesia Nomor : 1-144/KMA/SK/I/2011 tentang Pedoman Pelayanan Informasi di Pengadilan, Surat Keputusan Ketua Mahkamah Agung Republik Indonesia Nomor : 026/KMA/SK/II/2012 tentang Standar Pelayanan Peradilan, Mahkamah Agung RI membangun sebuah Sistem Informasi Penelusuran Perkara di

Pengadilan Militer II-09 Bandung yaitu SIPP Pengadilan Militer II-09 Bandung, seperti terlihat pada gambar 3.4 dan 3.5. Teknologi yang digunakan yaitu :

1. Sistem Informasi Penelusuran Perkara Pengadian Militer II-09 Bandung atau sering disebut SIPP Pengadilan Militer II-09 Bandung Server Lokal dan Server Web.
2. *Internet*
3. *Access Point/WIFI*

3.1.5 Infrastruktur

Pada pengadilan Militer II-09 Bandung telah memiliki infrastruktur dari tata kelola teknologi informasi yang digunakan yaitu sebgai berikut :

1. *Computer hardware platforms*

   Infrastruktur terkait *computer hardware platforms* adalah komputer yng digunakan oleh *server* dan *client. Server* SIPP Pengadilan Militer II-09 Bandung digunakan untuk melayani akses oleh semua pengguna SIPP dan masing-masing pengguna diberikan hak akses ke sesuai dengan tupoksinya masing-masing. *Server* ini hanya yang digunakan untuk aplikasi SIPP sedangkan *server* yang lain digunakan untuk beberapa aplikasi lokal sebagai *supporting. Server* dikelola oleh Sub Bagian Perencanaan, Teknologi Informasi dan Pelaporan. Berikut ini pada table 3.1 daftar nama *server* dan komputer beserta laptop *client.*

Tabel 3.1 Daftar *Server* dan *Clients*

No.	Nama Komputer	Spesifikasi Komputer	Sistem Operasi	Ket
1.	SIPP	a. *Processor* Intel® Pentium® 1.0 GHz b. *Memory* 2 GB c. *Hard Disk* 150 GB	Centos	
2.	Personal Komputer	a. *Processor* Intel® Core i5 b. *Memory* 2 GB c. *Hard Disk* 1 TB	Windows 10	
3.	Laptop	a. *Processor* Intel® Core i7 b. *Memory* 4 GB c. *Hard Disk* 1 GB	Windows 10	
4.	Siadilmil	-	Windows Server	
5.	Siratmil	a. *Processor* Intel® Pentium® 1.0 GHz b. *Memory* 2 GB c. *Hard Disk* 150 GB	Centos	
6.	Email Resmi	-	Google Apps	

2. *Operating system platforms*

   Sistem operasi yang digunakan pada infrastruktur komputer *server* dan *clients* seperti terlihat pada tabel 3.1 adalah Windows dan Linux.

3. *Enterprise and other software applications*

   Software adalah komponen infrastruktur yang dikelola oleh Sub Bagian Perencanaa, Teknologi Informasi dan Pelaporan, untuk kepentingan pelayanan SIPP di Pengadilan Militer II-09 Bandung. Berikut ini daftar *software* resmi yang dimiliki oleh Pengadilan Militer II-09 Bandung seperti pada tabel 3.4

Tabel 3.2 Daftar *Software* resmi dengan lisensi

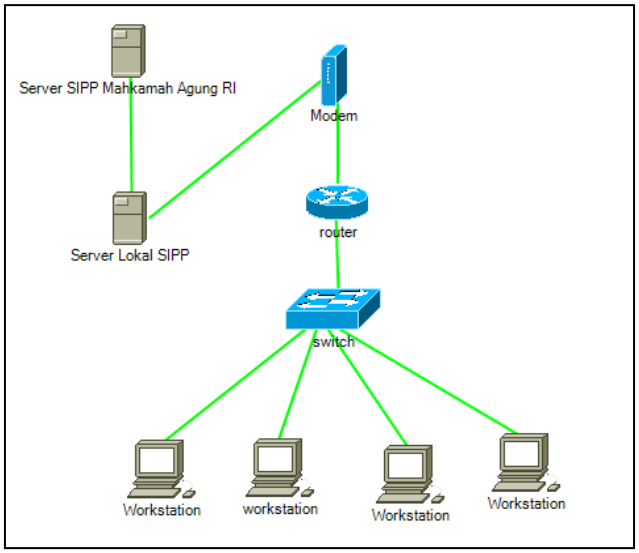
No.	Nama *Software*	Jenis Lisensi	Keterangan
1.	Microsoft Office	Microsoft Goverment	
2.	Kaspersky	Kaspersky License	
3.	SQLYog	Lisensi Mahkamah Agung RI	

4. *Data management and storage*

   Pada infrastruktur ini termasuk data dan informasi yang dikelola oleh *database management software* dan *storage device.* Teknologi peyimpanan yaitu pada *storage device* berupa harddisk eksternal dan *clouds* yaitu di google drive.

5. *Networking platforms*

   Teknologi jaringan komputer di internal topologi menggunakan TCP/IP dengan LAN dan WIFI. Serta untuk lalu lintas keamanan di jaringan, dibantu dengan menggunakan *hardware* berupa *router microtic.* Jaringan LAN berbasis ethernet serta jaringan LAN menggunakan WIFI/*Wireless.* Topologi yang digunakan adalah topologi star.



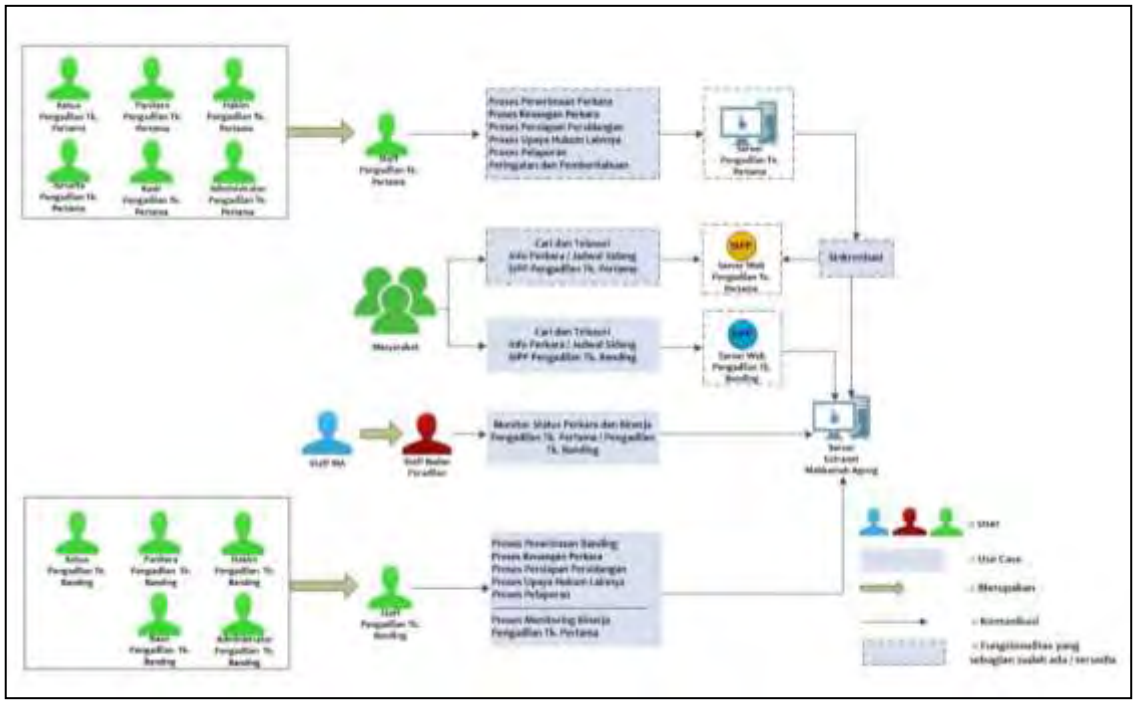
Gambar 3.3
Topologi Jaringan Pengadilan Militer II-09 Bandung

6. *Internet platforms*

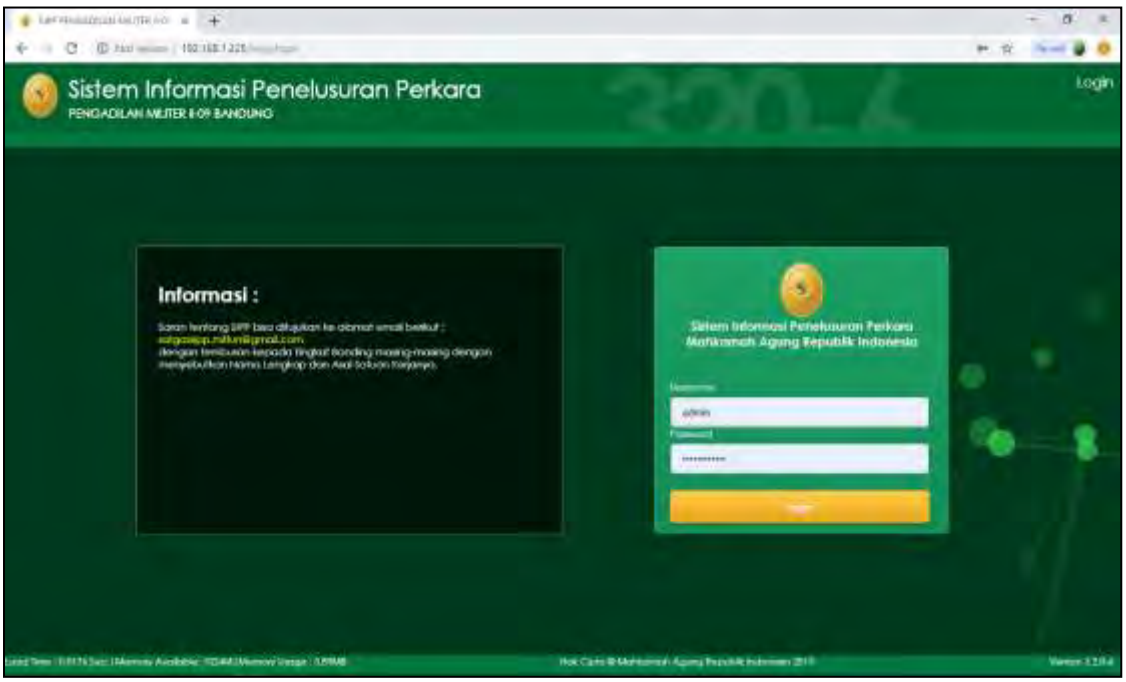
   Infrastruktur yang berkaitan termasuk didalamnya adalah *website domain* dan *hosting,* intranet dan internet. Jaringan LAN berbasis *Ethernet* dan *Wireless* menggunakan AstinetLite.

3.2 Sistem Informasi Penelusuran Perkara

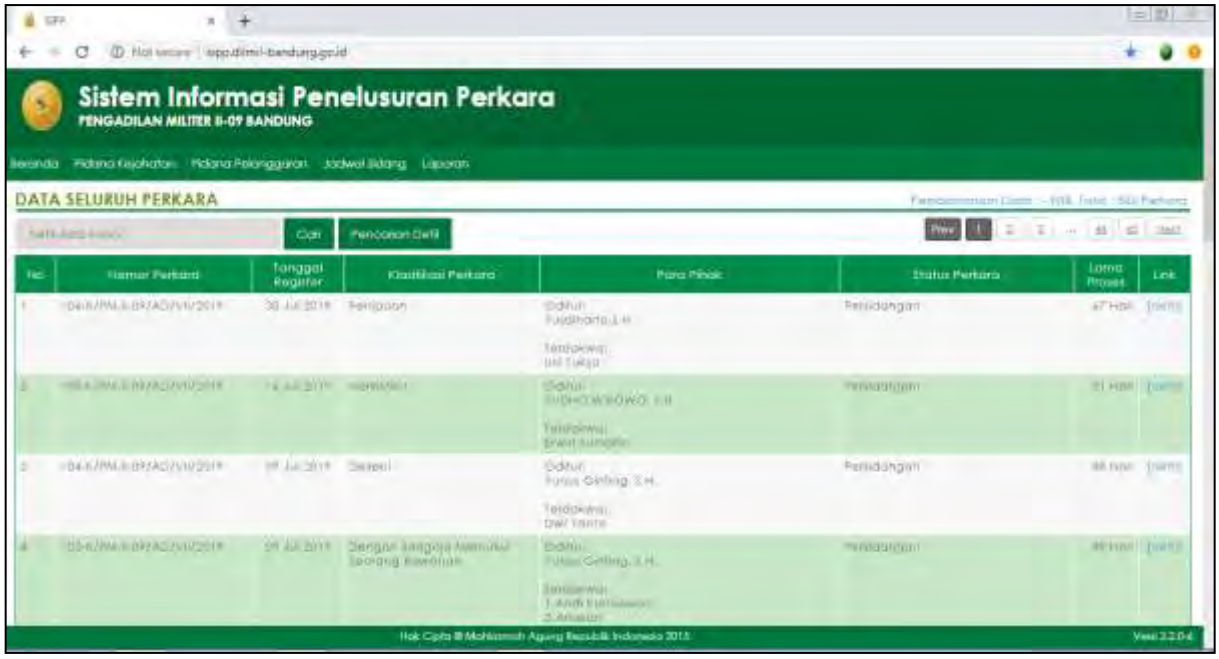
Aplikasi SIPP di Pengadilan Militer II-09 Bandung dikembangkan dengan satu *platform* terpadu di Mahkamah Agung RI berbasis *online.* SIPP yang digunakan di Pengadilan Militer II-09 Bandung ini terdiri dari 2 (dua) aplikasi utama yaitu SIPP Server Lokal dan SIPP Server Web. SIPP Pengadilan Militer II-09 Bandung membantu kinerja para penegak hukum di Pengadilan Militer II-09 Bandung dan masyarakat pencari keadilan untuk mengetahui dan memantau sampai sejauh mana keberlangsungan perkara yang dihadapi dan sedang berjalan.



Gambar 3.4
Arsitektur Sistem Informasi Penelusuran Perkara, (*Standard Operasional Procedure* Sistem Informasi Penelusuran Perkara)



Gambar 3.5
Sistem Informasi Penelusuran Perkara Server Lokal Pengadilan Militer II-09 Bandung



Gambar 3.6
Sistem Informasi Penelususran Perkara Server Web Pengadian Militer II-09 Bandung

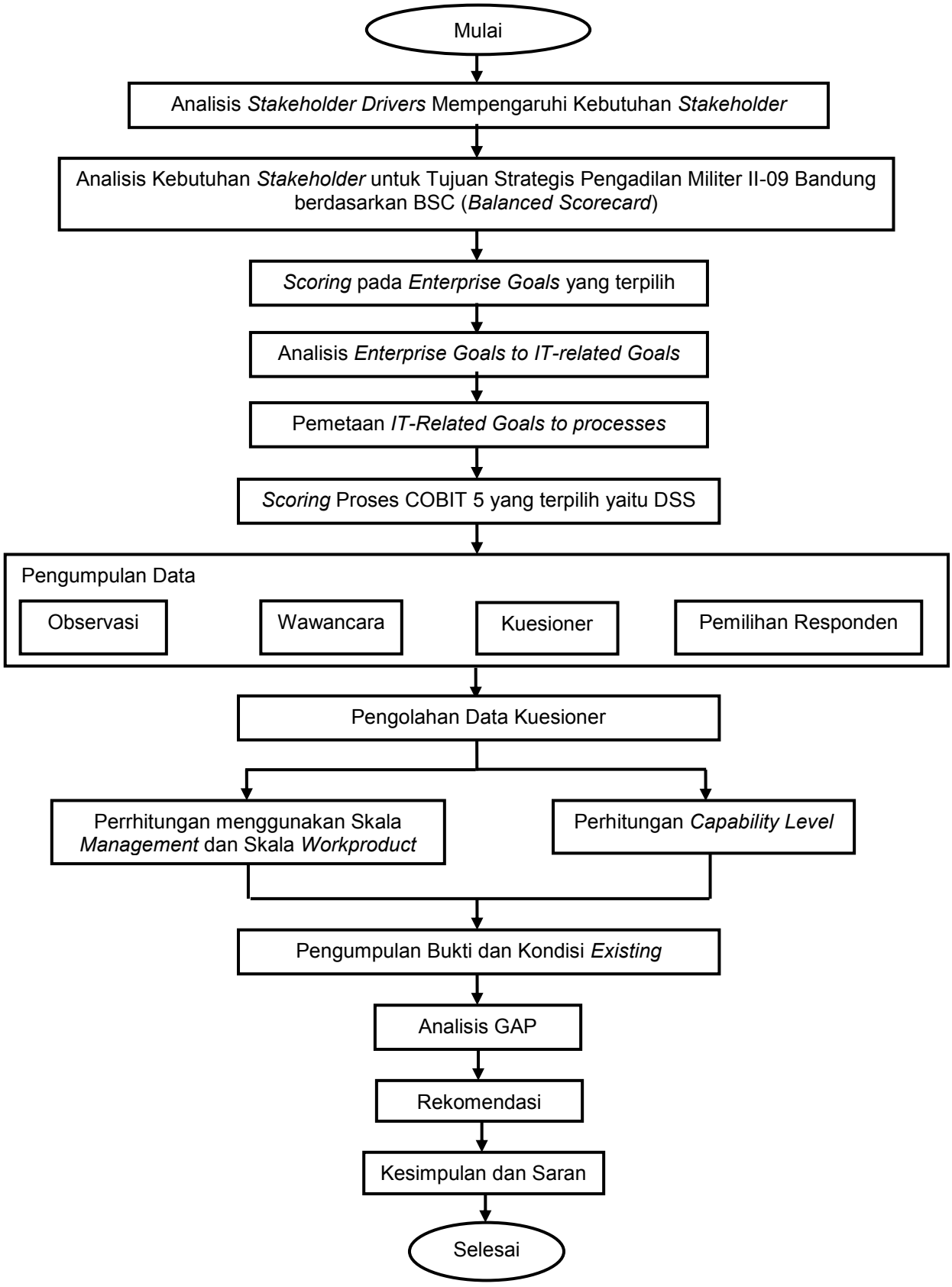
3.3 Metodologi Penellitian

Pengertian metodologi penelitian menurut Hidayat dan Sedarmayanti (2002:25) adalah pembahasan mengenai konsep teoritik berbagai metode, kelebihan dan kekurangan, yang dalam karya ilmiah dilanjutkan dengan pemilihan metode yang digunakan. Pengetian metodologi adalah “pengkajian terhadap langkah-langkah dalam menggunakan sebuah metode”.

Pada penelitian di Pengadilan Militer II-09 Bandung, metodologi penelitian yang digunakan adalah memulai, merumuskan masalah, studi literatur, pemetaan COBIT 5 dan ITIL V3 2011, pemilihan domain dan proses yang sesuai dengan penelitian, melakukan pengumpulan data dan dokumentasi, dengan wawancara dan kuesioner, mengolah dan menganalisis kuesioner, dengan menggunakan penilaian kapabilitas proses pada COBIT 5 berdasarkan pada ISO/IEC 15504, yaitu tingkat kapabilitas (*capability level*) dan analisis *gap dan* memberikan rekomendasi.

3.4 Alur Tahapan Penelitian

Penelitian ini terdiri dari beberapa tahapan, dimana keluaran ditahapan sebelumnya menjadi masukan pada tahapan berikutnya seperti telihat pada gambar 3.4



Gambar 3.7
Alur Tahapan Penelitian

Alur dari penelitian yang akan dilakukan oleh penulis :

1. Analisis *Stakeholder Drivers* Mempengaruhi Kebutuhan *Stakeholder*

   Kebutuhan *stakeholder* (pemangku kepentingan) dipengaruhi oleh sejumlah *driver*

2. Analisis Kebutuhan *Stakeholder* untuk Tujuan Strategis Pengadilan Militer II-09 Bandung berdasarkan BSC (*Balanced Scorecard*)

   Pada tahap pertama penelitian adalah mengidentifikasi tujuan strategis yang ada di Pengadilan Militer II-09 Bandung yang diperlukan untuk penggalian data kebutuhan *stakeholder* (*Stakeholder Need*) yang berhubungan dengan tujuan umum organisasi berdasarkan *BSC (Balanced Scoredcard)*.

3. *Scoring* pada *Enterprise Goals* yang terpilih

   Perhitungan *Enterprise Goals* yang terpilih dengan menggunakan teknik pengumpulan data melalui kuesioner.

4. Analisis *Enterprise Goals to IT-related Goals*

   Melakukan analisis terhadap *enterprise-Goals* yang terpilih *IT-related Goals* pada COBIT 5.

5. Pemetaan *IT-Related Goals to processes*

   Pada tahapan ini penulis melakukan pemeta tujuan strategis Pengadilan Militer II-09 Bandung pada COBIT 5.

6. Analisis *IT-Related Goals* pada COBIT 5 yang terpilih

   Menganalisis *IT-related Goals* yang telah terpilih pada tahap identifikasi.

7. Pemetaan *IT-Related Goals* to processes

   Pada tahap melakukan pemetaan *IT-Related Goals to processes* pada COBIT 5.

8. *Scoring* Proses COBIT 5 yang terpilih yaitu DSS

   Perhitungan melakukan scoring pada DSS01, DSS02, DSS03, DSS04, DSS05, dan DSS06 yang terpilih dengan menggunakan teknik pengumpulan data melalui kuesioner.

6. Pengumpulan Data

   Pada tahap dilakukan pengumpulan data pada domain terpilih pada COBIT 5 dan ITIL V3 2011 yang sesuai dengan permasalahan yang terkait layanan TI di

Pengadilan Militer II-09 Bandung yang relevan, yaitu dengan observasi, penyebaran kuesioner dan penentuan responden.

Pada penelitian ini pengumpulan data dilakukan dengan cara sebagai berikut :

a. Observasi

   Observasi dilakukan dengan tujuan untuk mengetahui keadaan nyata proses bisnis yang berhubungan dengan tata kelola teknologi informasi, infrastruktur teknologi informasi dan untuk mengetahui penggunaan infrstruktur tersebut.

b. Wawancara

   Wawancara adalah teknik pengumpulan data/informasi dari narasumber dengan melontarkan beberapa pertanyaan. Pada penelitian ini wawancara dilakukan untuk mengidentifikasi hal-hal yang berkaitan dengan kondisi Sistem Informasi Penelusuran Perkara, profil orgnisasi, visi misi organisasi dan data dukung lainnya.

c. Kuesioner

   Kuesioner adalah teknik mengumpulkan data dari sejumlah responden dengan daftar pertanyaan yang tertulis lalu diolah untuk menghasikan informasi yang utuh dan valid. Kuesioner dilakukan terhadap pengguna aplikasi Sistem Informasi Penelusuran Perkara, bagian yang melayani dan pendukung Sistem Informasi Penelusuran Perkar tersebut.

d. Pemilihan Responden

   Pada penyebaran kuesioner terlebih dahulu dilakukan penentuan responden yang mengacu pada diagram RACI (*Responsible, Accountable, Consulted, and/or Informed*) di COBIT 5 khususnya pada domain DSS (*Deliver, Service and Support*).

7. Perrhitungan menggunakan Skala *Management* dan Skala *Workproduct*

   Pada perhitungan kuesioner menggunakan teknik perhitungan skala *management* dan Skala *workproduct.*

8. Perhitungan *Capability Level*

   Pada tahap analisis, teknik analisis yang digunakan adalah *processes assessment*

model (PAM). PAM merupakan model pengukuran kapabilitas yang digunakan pada COBIT 5 dan satu-satunya model penilaian yang memberikan pandangan tingkat organisasi/perusahaan tentang kemampuan layanan TI, memberikan pandangan bisnis *end-to-end* tentang kemampuan TI untuk menciptakan nilai.

9. Rekomendasi

   Setelah memperoleh proses-proses yang menjadi prioritas perbaikan, maka setelah ini akan ditentukan rekomendasi perbaikan layanan berdasarkan kepada ITIL V3 2011 mengacu pada *mapping* dari COBIT 5.

10. Kesimpulan dan Saran

    Setelah memperoleh rekomendasi maka penulis akan menarik kesimpulan dan membuat saran.

BAB IV

ANALISIS DAN PEMBAHASAN PENELITIAN

4.1 Analisis *Stakeholder Drivers* Mempengaruhi Kebutuhan *Stakeholder*

Kebutuhan *stakeholder* (pemangku kepentingan) dipengaruhi oleh sejumlah *driver*, seperti perubahan strategi organisasi, perubahan kebijakan atau peraturan, perubahan teknologi terbaru dan lain-lain.

4.2 Analisis Kebutuhan *Stakeholder* untuk Tujuan Strategis Pengadilan Militer II-09 Bandung

Pada tahap ini dilakukan analisis tujuan strategis Pengadilan Militer II-09 Bandung berdasarkan kebutuhan *stakeholder* yang berhubungan dengan tujuan umum organisasi menggunakan dimensi *Balanced Scorecard (*BSC*)*. Dimensi *Balanced Scoredcard* (BSC) yang terdiri dari 4 (empat) perspektif utama yaitu *Financial, Customer, Internal Business Process* dan *Learning and Growth,* kemudian direlasikan dengan 17 (tujuh belas) *Enterprise Goals* dan dihubungkan dengan tujuan strategis Pengadilan Militer II-09 Bandung berdasarkan hubungan dengan tujuan dari *gorvernance* yaitu *Benefits Realitation* (Manfaat Realisasi), *Risk Optimisation* (Risiko Pengoptimalan) dan *Resource Optimisation* (Pengoptimalan Sumber Daya) seperti dijelaskan pada gambar 4.1

Tabel 4.1 Pemetaan *Enterprise Goals* to Tujuan Strategis (Indikator Tujuan) Pengadilan Militer II-09 Bandung

No.	Dimensi BSC	*Enterprise Goals*	*Relation to Governance Objective*			Tujuan Organisasi Pengadilan Militer II-09 Bandung
			Benefits Realitation	*Risk Optimisation*	*Resource Optimisation*	
1	*Financial*	1. *Stakeholder value of business investments (*nilai pemangku kebijakan dilihat dari investasi bisnis*)*	P		S	-
		*2. Portofolio of competitive products and service (*Portofolio produk dan layanan*)*	P	P	S	-
		*3. Managed business risk (safeguarding of asstes) (*Pengelolaan risiko bisnis / menjaga aset*)*		P	S	-
		*4. Compliance with external laws and regulations (*Kepatuhan dengan hukum dan peraturan eksternal*)*		P	S	-
		*5. Financial transparency (*Transparansi keuangan*)*	P	S	S	Peningkatan Pengelolaan Aset, Keuangan dan Kinerja
2	*Customer*	6. *Customer oriented service culture* (berorientasi pada pelanggan)	P		S	Terwujudnya pelayanan prima bagi masyarakat pencari keadilan
		7. *Business service continuity and availability (*keberlanjutan dan ketersediaan layanan*)*		P		-
		8. *Agile response to a changing business environment (*Respon cepat terhadap lingkungan bisnis yang berubah*)*	P		S	-

No.	Dimensi BSC	*Enterprise Goals*	*Relation to Governance Objective*			Tujuan Organisasi Pengadilan Militer II-09 Bandung
			Benefits Realitation	*Risk Optimisation*	*Resource Optimisation*	
		*9. Information-based strategic decision making (*Pengambilan keputusan strategis berdasarkan informasi*)*	P	P	P	-
		10. *Optimisation of service delivery costs(*Optimasi biaya pengiriman layanan*)*	P		P	-
3	*Internal Business Process*	11. *Optimisation of business process functionality (*Optimasi fungsionalitas proses bisnis*)*	P		P	Terwujudnya percepatan proses penanganan perkara melalui pemanfaatan teknologi informasi
		12. *Optimisation of business process costs (*Optimasi biaya proses bisnis*)*	P		P	-
		13. *Managed business change programmes (*Pengelolaan perubahan program bisnis*)*	P	P	S	-
		14. *Operational and staff productivity (*Produktivitas operasional dan staf*)*	P		P	-
		15. *Compliance with internal policies (*Kepatuhan terhadap kebijakan internal*)*		P		-
4	*Learning and Growth*	16. *Skilled and motivated people (*Kemampuan terampil dan termotivasi*)*	S	P	P	Terwujudnya pelayanan prima bagi masyarakat pencari keadilan
		17. *Product and business innovation culture (*Inovasi produk dan bisnis*)*	P			

Pada tabel 4.1 tersebut dijelaskan mengenai keterkaitan *Enterprise Goals* yang menggunakan *Balanced Scorecard* (BSC) pada COBIT 5 serta hubungan tujuan organisasi dilihat dari 3 (tiga) tujuan yaitu *benetifs realitation, risk optimisation* dan *resource optimisation* dimana P singkatan dari Primer artinya hubungan kuat dan S singkatan dari sekunder yang berarti hubungan kurang kuat atau berupa pendukung, kemudian berelasi dengan Tujuan Organisasi pada Pengadilan Militer II-09 Bandung. Selanjutnya akan dilakukan pemetaan antara keterhubungan *Entreprise Goals* dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yang mengacu berdasarkan Rencana Strategis (Renstra Pengadilan Militer II-09 Bandung) pada tabel 4.2

Tabel 4.2 Analisis Keterhubungan *Enterprise Goals* COBIT 5 dengan Tujuan Strategis Pengadilan Militer II-09 Bandung

No.	Dimensi BSC	Kode *Enterprise Goals*	*Enterprise Goals*	Hasil Pemetaan
1.	*Financial*	EG1	1. *Stakeholder value of business investments (*nilai pemangku kebijakan dilihat dari investasi bisnis*)*	1. Tidak Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG2	*2. Portofolio of competitive products and service (*Portofolio produk dan layanan*)*	2. Tidak Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG3	*3. Managed business risk (safeguarding of asstes) (*Pengelolaan risiko bisnis / menjaga aset*)*	3. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu Peningkatan Pengelolaan Aset, Keuangan dan Kinerja
		EG4	*4. Compliance with external laws and regulations (*Kepatuhan dengan hukum dan peraturan eksternal*)*	4. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung

No.	Dimensi BSC	Kode *Enterprise Goals*	*Enterprise Goals*	Hasil Pemetaan
		EG5	*5. Financial transparency (*Transparansi keuangan*)*	5. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu Peningkatan Pengelolaan Aset, Keuangan dan Kinerja
		EG6	6. *Customer oriented service culture* (berorientasi pada pelanggan)	6. Ada keterhubungan dengan Sasaran Strategis Pengadilan Militer II-09 Bandung yaitu Peningkatan aksebilitas masyarakat terhadap peradilan (*acces to justice*).
2.	*Customer*	EG7	7. *Business service continuity and availability (*keberlanjutan dan ketersediaan layanan*)*	7. Tidak ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG8	8. *Agile response to a changing business environment (*Respon cepat terhadap lingkungan bisnis yang berubah*)*	8. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu peningkatan percepatan proses penanganan perkara melalui pemanfaatan teknologi informasi
3.	*Internal Business Process*	EG9	*9. Information-based strategic decision making (*Pengambilan keputusan strategis berdasarkan informasi*)*	9. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu terwujudnya kepercayaan masyarakat terhadap sistem peradilan melalui proses peradilan yang pasti, transparan dan akuntabel.
		EG10	10. *Optimisation of service delivery costs (*Optimasi biaya pengiriman layanan*)*	10. Tidak Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG11	11. *Optimisation of business process functionality (*Optimasi fungsionalitas proses bisnis*)*	11. Tidak Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG12	12. *Optimisation of business process costs*	12. Ada keterhubungan dengan Tujuan

No.	Dimensi BSC	Kode *Enterprise Goals*	*Enterprise Goals*	Hasil Pemetaan
			*(*Optimasi biaya proses bisnis*)*	Strategis Pengadilan Militer II-09 Bandung yaitu peningkatan pelayanan peradilan dan mampu menjangkau seluruh lapisan masyarakat pencari keadilan.
		EG13	13. *Managed business change programmes (*Pengelolaan perubahan program bisnis*)*	13. Tidak Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung
		EG14	14. *Operational and staff productivity (*Produktivitas operasional dan staf*)*	14. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu pengembangan karir pegawai di Pengadilan Militer berupa Diklat-Diklat
		EG15	15. *Compliance with internal policies (*Kepatuhan terhadap kebijakan internal*)*	15. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yaitu proses kerja di internal berdasarkan tupoksi dan SOP (*Standard Opertional Procedure*) pada Sub Bagian masing-masing
4.	*Learning and Growth*	EG16	16. *Skilled and motivated people (*Kemampuan terampil dan termotivasi*)*	16. Ada keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung, yaitu pegawai dikut sertakan dalam TOT (*Training of Trainer*), Pelatihan dan Bimbingan Teknis, untuk meningkatkan tingkat kompetensi dan motivasi pegawai
		EG17	17. *Product and business innovation culture (*Inovasi produk dan bisnis*)*	17. Tidak ada keterhubungan dengan tujuan strategis Pengadilan Militer II-09 Bandung

Tabel 4.3 *Enterprise Goals Terpilih*

No.	Kode *Enterprise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Rencana Strategis Pengadilan Militer II-09 Bandung	
			Ada keterhubungan	Tidak Ada Keterhubungan
1.	EG1	1. *Stakeholder value of business investments (*nilai pemangku kebijakan dilihat dari investasi bisnis*)*		v
2.	EG2	2. *Portofolio of competitive products and service (*Portofolio produk dan layanan*)*		v
3.	EG3	3. *Managed business risk (safeguarding of asstes) (*Pengelolaan risiko bisnis / menjaga aset*)*	v	
4.	EG4	4. *Compliance with external laws and regulations (*Kepatuhan dengan hukum dan peraturan eksternal*)*	v	
5.	EG5	5. *Financial transparency (*Transparansi keuangan*)*	v	
6.	EG6	6. *Customer oriented service culture* (berorientasi pada pelanggan)	v	
7.	EG7	7. *Business service continuity and availability (*keberlanjutan dan ketersediaan layanan*)*		v
8.	EG8	8. *Agile response to a changing business environment (*Respon cepat terhadap lingkungan bisnis yang berubah*)*	v	
9.	EG9	9. *Information-based strategic decision making (*Pengambilan keputusan strategis berdasarkan informasi*)*	v	
10.	EG10	10. *Optimisation of service delivery costs (*Opti masi biaya pengiriman layanan*)*		v
11.	EG11	11. *Optimisation of business process functionality (*Optimasi fungsionalitas proses bisnis*)*		v
12.	EG12	12. *Optimisation of business process costs (*Optimasi biaya proses bisnis*)*	v	
13.	EG13	13. *Managed business change programmes (*Pengelolaan perubahan program bisnis*)*		v
14.	EG14	14. *Operational and staff productivity (*Produktivitas operasional dan staf*)*	v	
15.	EG15	15. *Compliance with internal policies (*Kepatuhan terhadap kebijakan internal*)*	v	

No.	Kode *Enterprise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Rencana Strategis Pengadilan Militer II-09 Bandung	
			Ada keterhubungan	Tidak Ada Keterhubungan
16.	EG16	16. *Skilled and motivated people (*Kemampuan terampil dan termotivasi*)*	v	
17.	EG17	17. *Product and business innovation culture (*Inovasi produk dan bisnis*)*		v

Hasil pemetaan *Enterprise Goals* terpilih yang ada keterhubungan dengan rencana Strategis Pengadilan Militer II-09 Bandung ada 10 (sepuluh) *Enterprise Goals* yang terhubung dan 7 (tujuh) yang tidak terhubung dengan Tujuan Strategis Pengadilan Militer II-09 Bandung.

4.3 *Scoring* pada *Enterprise Goals* yang terpilih

Selanjutnya setelah dilakukan pemetaan dan dari *Enterprise Goals* ke Tujuan Strategis Pengadilan Militer II-09 Bandung, tahap yang akan dilakukan adalah melakukan *scoring* pada pemetaan diatas berdasarkan tingkat kepentingan dengan responden sebanyak 10 (sepuluh) orang yang merupakan bagian dari manajemen dan pelaksana di Pengadilan Militer II-09 Bandung.

Tabel 4.4 Data Responden *Scoring* pada *Enterprise Goals* yang terpilih

No.	Responden	Jumlah Responden
1.	Hakim	2
2.	Sekretaris	1
3.	Panitera Pengganti	1
4.	Staf Pelaksana Perencanaan, TI dan Pelaporan	2
5.	Staf Pelaksana Panmud Pidana	2
6.	Staf Pelaksana Panmud Hukum	2

Pada *scoring* berdasarkan tingkat kepentingan untuk *Enterprise Goals* COBIT 5 dengan Tujuan Strategis Pengadilan Militer II-09 Bandung, menggunakan metode *skala likert,* seperti yang terlihat pada tabel 4.5

Tabel 4.5 *Skala Likert* untuk scoring tingkat kepentingan

Skala	*Score*	Tingkat Kepentingan
1	1-2	Tidak Penting
2	3-4	Sedikit Penting
3	5-6	Cukup Penting
4	7-8	Penting
5	9-10	Sangat Penting

Kemudian data dari responden tersebut diolah dan dilakukan *scoring* terhadap *Enterprise Goals* pada tabel 4.6

Tabel 4.6 Rekapitulasi *Scoring* terhadap *Enterprise Goals*

No.	Kode *Enter-prise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung		Skala										Rata-rata	Skor
			Ada	Tidak Ada	Hakim 1	Hakim 2	Sek-retaris	PP	Staf Pelak-sana PTIP	Staf Pelak-sana PTIP	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Hukum	Staf Pelak-sana Panmud Hukum		
1	EG1	Stakeholder value of business investments (nilai pemangku kebijakan dilihat dari investasi bisnis)		v	1	1	1	1	1	1	1	1	1	1	1	1
2	EG2	*Portofolio of competitive products and service* (Portofolio produk dan layanan)		v	1	1	1	1	1	1	1	1	1	1	1	1
3	EG3	*Managed business risk (safeguarding of asstes)* (Pengelolaan risiko bisnis / menjaga aset)	v		7	7	8	7	8	8	8	8	8	8	7,70	7
4	EG4	*Compliance with external laws and regulations* (Kepatuhan dengan hukum dan peraturan eksternal)	v		9	8	8	8	8	8	8	8	8	8	8,10	8

No.	Kode *Enter-prise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung		Skala										Rata-rata	Skor
			Ada	Tidak Ada	Hakim 1	Hakim 2	Sek-retaris	PP	Staf Pelak-sana PTIP	Staf Pelak-sana PTIP	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Hukum	Staf Pelak-sana Panmud Hukum		
5	EG5	*Financial transparency* (Transparansi keuangan)	v		8	8	9	8	8	9	8	8	8	8	8,20	8
6	EG6	*Customer oriented service culture* (berorientasi pada pelanggan)	v		7	1	8	7	8	7	8	8	1	1	1	7
7	EG7	*Business service continuity nd availability* (keberlanjutan dan ketersediaan layanan)		v	1	7	1	1	1	1	1	1	8	8	7,60	1
8	EG8	*Agile response to a changing business environment* (Respon cepat terhadap lingkungan bisnis yang berubah)	v		8	8	8	8	8	8	8	8	8	8	8,00	8
9	EG9	*Information-based strategic decision making* (Pengambilan keputusan strategis berdasarkan informasi)	v		8	8	8	8	8	8	8	8	8	8	8,00	8

No.	Kode *Enter-prise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung		Skala										Rata-rata	Skor
			Ada	Tidak Ada	Hakim 1	Hakim 2	Sek-retaris	PP	Staf Pelak-sana PTIP	Staf Pelak-sana PTIP	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Hukum	Staf Pelak-sana Panmud Hukum		
10	EG10	*Optimisation of service delivery costs* (Opti masi biaya pengiriman layanan)		v	1	1	1	1	1	1	1	1	1	1	1	1
11	EG11	*Optimisation of business process functionality* (Optimasi fungsionalitas proses bisnis)		v	1	1	1	1	1	1	1	1	1	1	1	1
12	EG12	*Optimisation of business process costs* (Optimasi biaya proses bisnis)	v		9	8	9	8	8	8	8	8	8	7	8,10	8
13	EG13	*Managed business change programmes* (Pengelolaan perubahan program bisnis)		v	1	1	1	1	1	1	1	1	1	1	1	1
14	EG14	*Operational and staff productivity* (Produktivitas operasional dan staf)	v		9	8	9	8	8	8	8	8	8	8	8,20	8

No.	Kode *Enter-prise Goals*	Deskripsi *Enterprise Goals*	Keterhubungan dengan Tujuan Strategis Pengadilan Militer II-09 Bandung		Skala										Rata-rata	Skor
			Ada	Tidak Ada	Hakim 1	Hakim 2	Sek-retaris	PP	Staf Pelak-sana PTIP	Staf Pelak-sana PTIP	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Hukum	Staf Pelak-sana Panmud Hukum		
15	EG15	*Compliance with internal policies* (Kepatuhan terhadap kebijakan internal)	v		9	8	8	8	8	8	8	8	8	8	8,10	8
16	EG16	*Skilled and motivated people* (Kemampuan terampil dan termotivasi)	v		8	8	9	8	8	8	8	8	8	8	8,10	8
17	EG17	*Product and business innovation culture* (Inovasi produk dan bisnis)		v	1	1	1	1	1	1	1	1	1	1	1	1

4.4 Analisis *Enterprise Goals to IT-related Goals*

Pada tahap ini dilakukan pemetaan dari *Enterprise Goals* terhadap *IT-Related Goals.* Pencapaian tujuan organisasi menurut COBIT 5 membutuhkan sejumlah hasil yang terkait dengan TI, yang diwakili oleh *IT-Related Goals*. *IT-Related* merupakan singkatan untuk informasi dan teknologi yang terkait, dan *IT-Related Goals* disusun berdasarkan dimensi IT *Balanced Scorecard* (IT BSC).

Tabel 4.7 Pemetaan *Enterprise Goals* terhadap *IT-Related Goals*

			Enterprise Goals																
			Stakeholder value of business investments	*Portfolio of competitive products and services*	*Managed business risk (safeguarding of assets)*	*Compliance with external laws and regulations*	*Financial transparency*	*Customer-oriented service culture*	*Business service continuity and availability*	*Agile responses to a changing business environment*	*Information-based strategic decision making*	*Optimisation of service delivery costs*	*Optimisation of business process functionality*	*Optimisation of business process costs*	*Managed business change programmes*	*Operational and staff productivity*	*Compliance with internal policies*	*Skilled and motivated people*	*Product and business innovation culture*
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
IT-Related Goals			***Financial***					***Customer***					***Internal***					***Learning and Growth***	
Financial	01	*Alignment of IT and business strategy*	P		S			P	S	P	P	S	P	S	P			S	S
	02	*IT compliance and support for business compliance with external laws and regulations*			S	P											P		
	03	*Commitment of executive management for making IT-related decisions*	P	S	S					S	S		S		P			S	S
	04	*Managed IT-related business risk*			P	S			P	S		P			S		S	S	
	05	*Realised benefits from IT-enabled investments and services portfolio*	P	P				S		S		S	S	P		S			S
	06	*Transparency of IT costs, benefits and risk*	S		S		P				S	P		P					
Customer	07	*Delivery of IT services in line with business requirements*	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	*Adequate use of applications, information and technology solutions*	S	S	S			S	S		S	S	P	S		P		S	S

			Enterprise Goals																
			Stakeholder value of business investments	*Portfolio of competitive products and services*	*Managed business risk (safeguarding of assets)*	*Compliance with external laws and regulations*	*Financial transparency*	*Customer-oriented service culture*	*Business service continuity and availability*	*Agile responses to a changing business environment*	*Information-based strategic decision making*	*Optimisation of service delivery costs*	*Optimisation of business process functionality*	*Optimisation of business process costs*	*Managed business change programmes*	*Operational and staff productivity*	*Compliance with internal policies*	*Skilled and motivated people*	*Product and business innovation culture*
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
IT-Related Goals			**Financial**					**Customer**					**Internal**					**Learning and Growth**	
Internal	09	*IT Agility*	S	P	S			S		P			P		S	S		S	P
	10	*Security of information, processing infrastructure and applications*			P	P			P								P		
	11	*Optimisation of IT assets, resources and capabilities*	P	S						S		P	S	P	S	S			S
	12	*Enablement and support of business processes by integrating applications and technology into business processes*	S	P	S			S		S		S	P	S	S	S			S
	13	*Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards*	P	S	S			S				S		S	P				
	14	*Availability of reliable and useful information for decision making*	S	S	S	S			P		P		S						
	15	*IT compliance with internal policies*			S	S											P		
Learning and Growth	16	*Competent and motivated business and IT personnel*	S	S	P			S		S						P		P	S
	17	*Knowledge, expertise and initiatives for business innovation*	S	P				S		P	S		S		S			S	P

Pada tabel 4.8 akan menggambarkan hasil pemetaan antara *Enterprise Goals* yang terpilih dengan Tujuan Strategis Pengadilan Militer II-09 Bandung yang dipetakan dengan *IT-Related Goals* dengan berdasarkan tabel 4.7

Tabel 4.8 Pemetaan *Enterprise-Goals* terhadap *IT-Related Goals* COBIT 5

No.	Kode *Enterprise Goals*	Pemetaan *Enterprise-Goals* terhadap *IT-Related Goals* COBIT 5	
		Ada Keterhubungan	*IT-Related Goals*
1.	EG3	V	4, 10, 16
2.	EG4	V	2, 10
3.	EG5	V	6
4.	EG6	V	1, 7
5.	EG8	V	1, 4, 10, 14
6.	EG9	V	1, 14
7.	EG12	V	5, 6, 11
8.	EG14	v	8, 16
9.	EG15	v	2, 10, 15
10.	EG16	v	16

Hasil dari pemetaan *Enterprise Goals* terhadap *IT-Related Goals* dijelaskan pada tabel 4.9

Tabel 4.9 *IT-Related Goals* Terpilih

No.	Kode *IT-Related Goals*	*IT-Related Goals*
1.	*IT-G1*	*Alignment of IT and business strategy* (Penyelarasan TI dan Strategi Bisnis)
2.	*IT-G2*	*IT compliance and support for business compliance with external laws and regulations* (Kepatuhan dan dukungan TI untuk kepatuhan bisnis dengan hukum dan peraturan eksternal)
3.	*IT-G4*	*Managed IT-related business risk* (Risiko bisnis *IT-related* dikelola)
4.	*IT-G5*	*Realised benefits from IT-enabled investments and services portfolio* (Realisasi manfaat dari TI memungkinkan investasi dan portofolio layanan)
5.	*IT-G6*	*Transparency of IT costs, benefits and risk* (Transparansi biaya, manfaat, dan risiko TI)

No.	Kode *IT-Related Goals*	*IT-Related Goals*
6.	*IT-G7*	*Delivery of IT services in line with business requirements* (Pengiriman layanan TI sesuai dengan persyaratan bisnis)
7.	*IT-G8*	*Adequate use of applications, information and technology solutions* (Penggunaan aplikasi, informasi, dan solusi teknologi yang memadai)
8.	*IT-G10*	*Security of information, processing infrastructure and applications* (Keamanan informasi, infrastruktur pemrosesan dan aplikasi)
9.	*IT-G11*	*Optimisation of IT assets, resources and capabilities* (Optimalisasi aset, sumber daya, dan kemampuan TI)
10.	*IT-G12*	*Enablement and support of business processes by integrating applications and technology into business processes* (Pemberdayaan dan dukungan proses bisnis dengan mengintegrasikan aplikasi dan teknologi ke dalam proses bisnis)
11.	*IT-G14*	*Availability of reliable and useful information for decision making* (Ketersediaan informasi yang andal dan bermanfaat untuk pengambilan keputusan)
12.	*IT-G15*	*IT compliance with internal policies* (Kepatuhan TI dengan kebijakan internal)
13.	*IT-G16*	*Competent and motivated business and IT personnel* (Personel bisnis dan TI yang kompeten dan bermotivasi)

Dari hasil pemetaan *Enterprise Goals* dengan *IT-Related Goals* didapatkan 13 (tiga belas) *IT-Related Goals* yang terpilih.

4.5 Pemetaan *IT-Related Goals to processes*

Setelah *IT-Related Goals* terpilih kemudian *IT-Related Goals* tersebut dilakukan pemetaan ke proses-proses di COBIT 5, seperti tergambar pada tabel 4.10

Tabel 4.10 Pemetaan COBIT 5 *IT-Related Goals to Processes*

			IT-Related Goals																
			Alignment of IT and business strategy	*IT compliance and support for business compliance with external laws and regulations*	*Commitment of executive management for making IT-related decisions*	*Managed IT-related business risk*	*Realised benefits from IT-enabled investments and services portfolio*	*Transparency of IT costs, benefits and risk*	*Delivery of IT services in line with business requirements*	*Adequate use of applications, information and technology solutions*	*IT Agility*	*Security of information, processing infrastructure and applications*	*Optimisation of IT assets, resources and capabilities*	*Enablement and support of business processes by integrating applications and technology into business processes*	*Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards*	*Availability of reliable and useful information for decision making*	*IT compliance with internal policies*	*Competent and motivated business and IT personnel*	*Knowledge, expertise and initiatives for business innovation*
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
COBIT 5 *Process*			***Financial***						***Customer***		***Internal***							***Learning and Growth***	
Deliver, Service and Support	DSS01	*Manage Operations*		S		P	S		P	S	S	S				S	S	S	S
	DSS02	*Manage Service Requests and Incidents*				P			P	S		S				S	S		S
	DSS03	*Manage Problems*		S		P	S		P	S	S		P	S		P	S		S
	DSS04	*Manage Continuity*	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	*Manage Security Services*	S	P		P			S	S		P	S	S		S	S		
	DSS06	*Manage Business Process Controls*		S		P			P	S		S	S	S		S	S	S	S

Pada tabel 4.10 pemetaan *IT-Related Goals* COBIT 5 to *processes,* diperoleh dari nilai P (Primer) yang berarti bahwa data tersebut sangat penting sedangkan untuk nilai S (Sekunder) dijadikan data pendukung. Kemudian dipilih proses-proses berdasarkan *IT-Related Goals* yang terpilih pada domain DSS01 sampai dengan DSS06.

4.6 *Scoring* Proses COBIT 5 yang terpilih yaitu DSS

Selanjutnya setelah dilakukan pemetaan dan dari *IT-Related Goals* ke Proses COBIT 5 yaitu domain yang terpilih yaitu DSS sesuai dengan permasalahan yang ada di

Pengadilan Militer II-09 Bandung terkait layanan TI. Kemudian melakukan *scoring* pada DSS01, DSS02, DSS03, DSS04, DSS05, dan DSS06 seperti yang tersebut pada tabel 4.10 dibawah berdasarkan tingkat kepentingan dengan responden sebanyak 10 (sepuluh) orang yang merupakan bagian dari manajemen di Pengadilan Militer II-09 Bandung.

Tabel 4.11 Data Responden pada *Scoring* Proses COBIT 5 yang terpilih yaitu DSS

No.	Responden	Jumlah Responden
1.	Hakim	2
2.	Sekretaris	1
3.	Panitera Pengganti	1
4.	Staf Pelaksana Perencanaan, TI dan Pelaporan	2
5.	Staf Pelaksana Panmud Pidana	2
6.	Staf Pelaksana Panmud Hukum	2

Pada *scoring* berdasarkan tingkat kepentingan untuk DSS01, DSS02, DSS03, DSS04, DSS05 dan DSS06 pada COBIT 5 menggunakan metode *skala likert,* seperti yang terlihat pada tabel 4.12

Tabel 4. 12 *Skala Likert* untuk *scoring* tingkat kepentingan

Skala	*Score*	Tingkat Kepentingan
1	1-2	Tidak Penting
2	3-4	Sedikit Penting
3	5-6	Cukup Penting
4	7-8	Penting
5	9-10	Sangat Penting

Kemudian data dari responden tersebut diolah dan dilakukan *scoring* terhadap *Enterprise Goals* pada tabel 4.13

Tabel 4. 13 Rekapitulasi *Scoring* COBIT 5 *IT-Related Goals to Processes*

Deliver, Service and Support		Skala										Rata-rata	Skor
		Hakim 1	Hakim 2	Sekretaris	Panitera Pengganti	Staf Pelak-sana PTIP	Staf Pelak-sana PTIP	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Pidana	Staf Pelak-sana Panmud Hukum	Staf Pelak-sana Panmud Hukum		
DSS01	*Manage Operations*	8	8	8	7	8	7	8	9	8	8	7,90	7
DSS02	*Manage Service Requests and Incidents*	8	8	8	7	8	8	7	9	8	8	7,90	8
DSS03	*Manage Problems*	8	8	8	7	8	9	7	9	8	8	8,00	8
DSS04	*Manage Continuity*	7	8	8	7	8	7	7	8	8	8	7,60	7
DSS05	*Manage Security Services*	7	8	8	7	8	8	8	9	8	8	7,90	7
DSS06	*Manage Business Process Controls*	7	8	8	7	8	8	8	8	8	8	7,80	7

4.7 Pengumpulan Data

4.7.1 Observasi

Pengumpulan data pada penelitian ini yaitu pertama dengan melakukan observasi di Pengadilan Militer II-09 Bandung dengan tujuan untuk mengetahui keadaan terkait Sistem Informasi Penelusuran baik dari infrastruktur teknologi informasi dan permasalahan-permasalahan yang terjadi dengan Sistem Informasi Penelusuran Perkara dan menelaah bukti yang diperoleh. Dan bukti tersebut merupakan menjadi hasil yang valid untuk temuan bukti dan permasalahan dalam penelitian.

Tabel 4.14 Dokumen Pendukung Penelitian

No.	Nama Dokumen
1.	SOP Sistem Informasi Penelusuran Perkara
2.	SOP Pemeliharaan Sistem Informasi Penelusuran Perkara
3.	SOP Penanganan *Hardware*/Pengolahan Data
4.	Berita Acara Penanganan *Hardware*/Pengolahan Data Rusak
5.	Berita Acara Penanganan Permasalahan Terkait Sistem Informasi Penelusuran Perkara
6.	Rekapitulasi Penanganan Permasalahan Sistem Informasi Penelusuran Perkara
7.	Laporan Pengecekan dan Pembaharuan Data Sistem Informasi Penelusuran Perkara
8.	Laporan Pengecekan Infrastruktur IT
9.	*Billing* dengan pihak ketiga (Qwords Hosting)
10.	*Billing* dengan pihak ketiga (pembelian Antivirus)
11.	Kontrak dengan Astinet Lite
12.	Laporan Hakim Pengawas Bidang Perencanaan, Teknologi Informasi dan Pelaporan Pengadilan Militer II-09 Bandung Periode Januari sampai dengan Mei 2019

Dokumen yang terkait dalam penelitian ini yang tersebut pada table 4.13 diatas akan digunakan sebagai bahan acuan dalam penetapan proses *Capability Level* terutama pada domain DSS (*Deliver, Service and Support*), Sub Domain DSS01, DSS02, DSS03, DSS04, DSS05 dan DSS06.

4.7.2 Wawancara

Pada penelitian ini selain melakukan observasi, untuk mengumpulkan bukti dilakukan wawancara kepada responden secara langsung yaitu dari pihak manajerial yaitu Sekretaris Pengadilan Militer II-09 Bandung. Tujuan wawancaranya adalah untuk mengkonfirmasi keselarasan atas hasil proses pada TI dan Sistem Informasi Penelusuran Perkara untuk menentukan target *Capability Level* pada domain DSS COBIT 5 di Pengadilan Militer II-09 Bandung.

4.7.3 Kuesioner

Penyusunan kuesioner disusun berdasarkan standar *framework* COBIT 5 domain DSS direlasikan dengan standar ITIL V3 2011. Kuesioner ini digunakan untuk menilai sejauh mana proses layanan TI telah dicapai oleh Pengadilan Militer II-09 Bandung.

Formulir kuesioner berisi daftar pertanyaan pada domain DSS01, DSS02, DSS03, DSS04, DSS05, dan DSS06 pada COBIT 5 yang berelasi dengan proses pada ITIL V3 2011. Setelah didapat jawaban dari hasil kuesioner dapat dianalisis dan dijadikan proses audit.

Formulir kuesioner terdiri dari :

1. Judul Kuesioner
2. Proses Domain DSS COBIT 5 yang berelasi proses di ITIL V3 2011
3. Terkait Standar : ITIL V3 2011
4. Identitas Responden berupa Nama dan Jabatan/Posisi.
5. Tata Cara Pengisian
6. Tabel Pertanyaan.

4.7.4 Pemilihan Responden

Peran pada diagram RACI selanjutnya dipetakan kepada peran-peran yang terkait pada struktur organisasi di Pengadilan Militer II-09 Bandung yang terkait dengan COBIT 5 domain DSS, dimana diharapkan akan mendapatkan jawaban dari kuesioner dan mewakili evaluasi Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung.

Tabel 4.15 Daftar *stakeholder* terkait Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung

No.	Jabatan	Jumlah
1	Hakim	2
2	Sekretaris	1
3	Panitera Pengganti	1
4	Staf Pelaksana Perencanaan, TI dan Pelaporan	2
5	Staf Pelaksana Panmud Pidana	2
6	Staf Pelaksana Panmud Hukum	2
Jumlah		10

Dari tabel 4.15 diatas *stakeholder* yang terkait dengan Sistem Informasi Penelusuran Perkara akan menjadi responden untuk menjawab kuesioner pada domain DSS yang terdiri dari 2 (dua) orang Hakim, Sekretaris, Panitera Pengganti, 2 (dua) orang Staf Pelaksana Perencanaan, Teknologi Informasi dan Pelaporan, 2 (dua) orang Staf Pelaksana Panmud Pidana dan 2 (dua) orang Staf Pelaksana Panmud Hukum.

Selanjutnya penentuan responden mengacu ke diagram RACI (*Responsible, Accountable, Consulted and/or Informed*) pada COBIT 5 terutama pada domain DSS (*Deliver, Service and Support*). Peran-peran yang terdapat pada diagram RACI yaitu *stakeholder* yang terkait dengan proses-proses pada DSS. Setelah terlihat pada diagram RACI, kemudian dilakukan pemetaan ke struktur organisasi pada Pengadilan Militer II-09 Bandung. Berikut ini rincian responden berdasarkan diagram RACI pada domain DSS COBIT 5, yaitu :

Tabel 4. 16 Pemetaan Diagram RACI dengan Jabatan dalam struktur organisasi di Pengadilan Militer II-09 Bandung

No.	Diagram RACI	Jabatan
1	*Chief Operating Officer*	Sekretaris
2	*Chief Financial Officer*	Kasubag Umum dan Keuangan

No.	Diagram RACI	Jabatan
4	*Business Executive*	Hakim / Panitera / Panmud Pidana / Panitera Pengganti / Pelaksana Panmud Pidana / Pelaksana Panmud Hukum
5	*Business Process Owners*	Panitera, Sekretris
6	*Chief Risk Officer*	Pelaksana Subag Perencanaan, TI dan Pelaporan
7	*Chief Information Security Officer*	Pelaksana Subag Perencanaan, TI dan Pelaporan
8	*Chief Information Officer*	Kasubag Perencanaan, TI dan Pelaporan
9	*Head Human Resources*	Kasubag Kepegawaian dan Ortala
10	*Chief Information Officer*	Kasubag Perencanaan, TI dan Pelaporan
11	*Head IT Operations*	Kasubag Perencanaan, Teknologi Informasi dan Pelaporan / Pelaksana Subag Perencanaan, Teknologi Informasi dan Pelaporan
12	*Service Manager*	Pelaksana Subag Perencanaan, TI dan Pelaporan / Pelaksana Panmud Pidana
13	*Information Security Manager*	Pelaksana Subag Perencanaan, Teknologi Informasi dan Pelaporan
14	*Business Continuity Manager*	Panitera, Sekretaris

Pada tabel 4.16 tersebut menunjukkan berdasarkan standar COBIT 5 pada domain DSS terdapat 10 (sepuluh) *stakeholder* yang mempunyai peran dan terkait dengan struktur organisasi di Pengadilan Militer II-09 Bandung, namun pada jabatan tersebut yang terdapat pada struktur organisasi hanya ada 4 (empat) orang yang melaksanakan tugas sesuai dengan RACI, dan beberapa orang yang merangkap tugas sesuai standar yang ada pada COBIT 5.

Tabel 4.17 Pemetaan Diagram RACI domain DSS COBIT 5

	Management Practice	Hakim	Sekretaris	Panitera Pengganti	Pelaksana Perencanaan, TI dan Pelaporan	Pelaksana Panmud Pidana	Pelaksana Panmud Hukum
DSS01	DSS01.01 *Perform operational procedures.*		C		AC		
	DSS01.02 *Manage outsourced IT services.*				RI		
	DSS01.03 *Monitor IT infrastructure.*		I		ACI		
	DSS01.04 *Manage the environment.*		I		RACI		
	DSS01.05 *Manage facilities.*		I		RACI		
DSS02	DSS02.01 *Define incident and service request classification schemes.*		C		RCI		
	DSS02.02 *Record, classify and prioritise requests and incidents.*				RA		
	DSS02.03 *Verify, approve and fulfill service requests.*				RAI		
	DSS02.04 *Investigate, diagnose and allocate incidents.*				RACI		
	DSS02.05 *Resolve and recover from incidents.*				RAI		
	DSS02.06 *Close service requests and incidents.*				RAI		
	DSS02.07 *Track status and produce reports.*				RAI		
DSS03	DSS03.01 *Identify and classify problems.*	I		I	RACI	I	I
	DSS03.02 *Investigate and diagnose problems.*				RACI		
	DSS03.03 *Raise known errors.*				RA		
	DSS03.04 *Resolve and close problems.*	I		I	RACI	I	I
	DSS03.05 *Perform proactive problem management.*				RAC		
DSS04	DSS04.01 *Define the business continuity policy, objectives and scope*	C	RA	C	RACI	C	C
	DSS04.02 *Maintain a continuity strategy.*	C	RA	C	RCI	C	C
	DSS04.03 *Develop and implement a business continuity response.*	I	A	I	RC	I	I
	DSS04.04 *Exercise, test and review the BCP.*	I	A	I	R	I	I
	DSS04.05 *Review, maintain and improve the continuity plan.*	I	RA	I	RCI	I	I
	DSS04.06 *Conduct continuity plan training.*	I	A	I	RCI	I	I
	DSS04.07 *Manage backup arrangements.*		R		AC		
	DSS04.08 *Conduct post-resumption review.*	C	A	C	RCI	C	C

Management Practice		Hakim	Sekretaris	Panitera Pengganti	Pelaksana Perencanaan, TI dan Pelaporan	Pelaksana Panmud Pidana	Pelaksana Panmud Hukum
DSS05	DSS05.01 *Protect against malware.*				RACI		
	DSS05.02 *Manage network and connectivity security.*				RACI		
	DSS05.03 *Manage endpoint security.*				RACI		
	DSS05.04 *Manage user identity and logical access.*				RACI		
	DSS05.05 *Manage physical access to IT assets.*				RACI		
	DSS05.06 *Manage sensitive documents and output devices.*				RI		
	DSS05.07 *Monitor the infrastructure for security-related events.*		I		RACI		
DSS06	DSS06.01 *Align control activities embedded in business processes with enterprise objectives*	A	C	A	CI	A	A
	DSS06.02 *Control the processing of information.*	A	R	A	CI	A	A
	DSS06.03 *Manage roles, responsibilities, access privileges and levels of authority.*	A		A	RCI	A	A
	DSS06.04 *Manage errors and exceptions.*	I	I	I	RC	I	I
	DSS06.05 *Ensure traceability of information events and accountabilities.*	C		C	CI	C	C
	DSS06.06 *Secure information assets.*	C	C	C	CI	C	C

Pada tabel 4.17 RACI mempunyai arti sebagai berikut :

1. R (*Responsible)* pihak yang bertanggung jawab melaksanakan pekerjaan.

b. A (*Accountable)* pihak yang bertanggung jawab pada suatu pekerjaan dan memiliki wewenang untuk memutuskan suatu permasalahan.

c. C (*Consulted)* pihak yang memberikan konsultasi.

d. I (*Informed)* pihak yang perlu mengetahui tindakan dan hasil ataupun keputusan yang telah diambil.

4.8 Pengolahan Data Kuesioner

Pada penelitian ini untuk melakukan pengolahan data kuesioner menggunakan metode *Process Assesment Model (*PAM*)* dan *Capability Level* pada COBIT 5 yaitu model untuk melakukan penilaian terhadap kemampuan proses TI di Pengadilan Militer II-09 Bandung terhadap COBIT 5. Kuesioner yang akan diolah mempunyai tujuan untuk mengetahui tingkat kapabilitas pengelolaan Sistem Informasi Penelusuran Perkara, yaitu dengan standar pertanyaan pada domain DSS di COBIT 5 yang direkasikan dengan standar proses di ITIL V3 2011.

4.8.1 Menghitung Proses dan *Output* DSS01

Pertanyaan yang diajukan kepada responden untuk sub domain DSS01 Mengelola prosedur operasional terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-aktivitas apa saja yang dilakukan pada proses DSS01 yaitu DSS01.01 melaksanakan prosedur operasional, DSS01.02 mengelola layanan TI *outsourcing*, DSS01.03 mengelola infrastruktur TI, DSS01.04 mengelola lingkungan dan DSS01.05 mengelola fasilitas-fasilitas, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Dari pertanyaan-pertanyaan yang disajikan pada kuesioner DSS01.01, DSS01.02, DSS01.03, DSS01.04 dan DSS01.05 maka dilakukan perhitungan berdasarkan *management practice* dan *output* yang dihasilkan pada proses DSS01 Isian kuesioner berisi “Ya” yang bernilai 1 dan “Tidak” bernilai 0.

Skala *Management Practice* = $\frac{479}{510}$ x 100% = 94%

Skala *Workproduct* = $\frac{89}{102}$ x 100% = 87%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS01 berdasarkan skala *management practice* dan skala *workprodct*, mulai dari DSS01.01, DSS01.02, DSS01.03, DSS01.04, dan DSS01.05, dapat dilihat pada tabel 4.18

Tabel 4.18 Hasil Pengolahan Data DSS01 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS01.01	Melaksanakan prosedur operasional	72	8	80	90%	18	2	20	90%	90%	F
DSS01.02	Mengelola layanan TI outsourcing	39	1	40	98%	8	2	12	83%	89%	F
DSS01.03	Mengelola infrastruktur TI	72	8	80	90%	26	4	30	87%	88%	F
DSS01.04	Mengelola lingkungan	86	4	90	96%	17	3	20	85%	90%	F
DSS01.05	Mengelola fasilitas-fasilitas	210	10	220	95%	18	2	20	90%	93%	F
Total		**479**	**31**	**510**	**94%**	**89**	**13**	**102**	**87%**	**90%**	**F**

Hasil kuesioner DSS01 Mengelola prosedur operasional pada *management practice* 94%, dan *output* hasilnya 87%, dengan skala rata-rata dari *management practice* dan *output* sebesar 90% dengan *rating* F (*Fully - Achieved*).

4.8.2 Menghitung Proses dan *Output* DSS02

Pertanyaan yang diajukan kepada responden untuk sub domain DSS02.01 Mengelola permintaan dan insiden layanan terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-aktivitas apa saja yang dilakukan pada proses DSS02 yaitu DSS02.01 mendefinisikan skema klasifikasi insiden dan permintaan layanan, DSS02.02 merekam, mengklasifikasikan, dan memprioritaskan permintaan dan insiden, DSS02.03 memverifikasi, menyetujui dan memenuhi permintaan, DSS02.04 menyelidiki, mendiagnosa dan mengalokasikan insiden, DSS02.05 menyelesaikan dan memulihkan insiden, DSS02.06 menyelesaikan dan memulihkan insiden dan DSS02.07 melacak status dan membuat laporan, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Dari pertanyaan-pertanyaan yang disajikan pada kuesioner DSS02.01, DSS02.02, DSS02.03, DSS02.04, DSS02.05, DSS02.06 dan DSS02.07 maka dilakukan perhitungan berdasarkan *management practice* dan *output* yang dihasilkan pada proses DSS02. Isian kuesioner berisi “Ya” yang bernilai 1 dan “Tidak” bernilai 0.

Skala *Management Practice* = $\frac{228}{250}$ x 100% = 91%

Skala *Workproduct* = $\frac{125}{140}$ x 100% = 89%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS02 berdasarkan skala *management practice* dan skala *workprodct*, mulai dari DSS02.01, DSS02.02, DSS02.03, DSS02.04, DSS02.05, DSS02.06 dan DSS02.07, dapat dilihat pada tabel 4.19

Tabel 4.19 Hasil Pengolahan Data DSS02 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS02.01	Mendefinisikan, Skema Klasifikasi Insiden dan Permintaan Layanan	43	7	50	86%	27	3	30	90%	88%	F
DSS02.02	Merekam, mengklasifikasikan, dan memprioritaskan permintaan dan insiden	27	3	30	90%	16	4	20	80%	85%	L
DSS02.03	Memverifikasi, menyetujui dan memenuhi permintaan	30	0	30	100%	18	2	20	90%	95%	F
DSS02.04	Menyelidiki, mendiagnosa dan mengalokasikan insiden	29	1	30	97%	19	1	20	95%	96%	F
DSS02.05	Menyelesaikan dan memulihkan insiden	38	2	40	95%	9	1	10	90%	93%	F
DSS02.06	Menyelesaikan dan memulihkan insiden	17	3	20	85%	18	2	20	90%	88%	F
DSS02.07	Melacak status dan membuat laporan	44	6	50	88%	18	2	20	90%	89%	F
Total		**228**	**22**	**250**	**91%**	**125**	**15**	**140**	**89%**	**90%**	**F**

Hasil kuesioner DSS02 Mengelola permintaan dan insiden layanan pada *management practice* sebesar 91%, dan *output* hasilnya 89%, dengan skala rata-rata dari *management practice* dan *output* sebesar 90% dengan *rating* F (*Fully - Achieved*).

4.8.3 Menghitung Proses dan *Output* DSS03

Pertanyaan yang diajukan kepada responden untuk sub domain DSS03 mengelola masalah terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-aktivitas apa saja yang dilakukan pada proses DSS03, yaitu DSS03.01 mengidentifikasi dan mengklasifikasikan masalah, DSS03.02 mengivestigasi dan mendiagnosis masalah, DSS03.03 kesalahan yang diketahui palsu, DSS03.04 mengatasi dan menutup masalah, dan DSS03.05 menjalankan manajemen masalah secara proaktif, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Selanjutnya dari pertanyaan-pertanyaan yang disajikan pada kuesioner DSS03.01, DSS03.02, DSS03.03, DSS03.04 dan DSS03.05 maka dilakukan perhitungan berdasarkan *management practice* dan *output* yang dihasilkan pada proses DSS03. Isian kuesioner berisi “Ya” yang bernilai 1 dan “Tidak” bernilai 0.

Skala *Management Practice* $\frac{225}{250}$ x 100% = 90%

Skala *Workproduct* $\frac{98}{111}$ x 100% = 89%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS03 berdasarkan skala *management practice* dan skala *workprodct*, mulai dari DSS03.01, DSS03.02, DSS03.03, DSS03.04, dan DSS03.05, dapat dilihat pada tabel 4.20

Tabel 4.20 Hasil Pengolahan Data DSS03 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS03.01	Mengidentifikasi dan mengklasifikasikan masalah	53	7	60	88%	27	3	30	90%	89%	F
DSS03.02	Mengivestigasi dan mendiagnosis masalah	33	7	40	83%	18	3	21	86%	84%	L
DSS03.03	Kesalahan yang diketahui palsu	28	2	30	93%	20	0	20	100%	97%	F
DSS03.04	Mengatasi dan menutup masalah	54	6	60	90%	17	3	20	85%	88%	F

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS03.05	Menjalankan manajemen masalah secara proaktif	57	3	60	95%	16	4	20	80%	88%	F
Total		**225**	**25**	**250**	**90%**	**98**	**13**	**111**	**88%**	**89%**	**F**

Hasil kuesioner DSS03 Mengelola masalah pada *management practice* 90%, dan *output* hasilnya 88%, dengan skala rata-rata dari *management practice* dan *output* sebesar 89% dengan *rating* F (*Fully - Achieved*).

4.8.4 Menghitung Proses dan *Output* DSS04

Pertanyaan yang diajukan kepada responden untuk sub domain DSS04 Mengelola kontinuitas terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-aktivitas apa saja yang dilakukan pada proses DSS04 yaitu DSS04.01 menetapkan kebijakan, tujuan dan ruang lingkup keberlanjutan bisnis, DSS04.02 mempertahankan strategi kontinuitas, DSS04.03, DSS04.04 pelatihan, pengujian dan peninjauan rencana berkelanjutan (BCP), DSS04.05 meninjau, memelihara dan meningkatkan rencana berkelanjutan, DSS04.06 melaksanakan pelatihan rencana berkelanjutan, DSS04.07 mengelola pengaturan back-up dan DSS04.08 melakukan review ulang, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Selanjutnya dari pertanyaan-pertanyaan yang disajikan pada kuesioner DSS04.01, DSS04.02, DSS04.03, DSS04.04, DSS04.05, DSS04.06, DSS04.07 dan DSS04.08 kemudian dihitung berdasarkan *management practice* dan *output* yang dihasilkan pada proses DSS04. Isian kuesioner berisi “Ya” yang bernilai 1 dan “Tidak” bernilai 0.

Skala *Management Practice* $\frac{379}{480}$ x 100% = 79%

Skala *Workproduct* $\frac{113}{320}$ x 100% = 35%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS04, mulai dari DSS04.01, DSS04.02, DSS04.03, DSS04.04, dan DSS04.05, DSS04.06, DSS04.07 dan DSS04.08 dapat dilihat pada tabel 4.21

Tabel 4. 21 Hasil Pengolahan Data DSS04 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS04.01	Menetapkan kebijakan, tujuan dan ruang lingkup keberlanjutan bisnis	93	7	100	93%	27	3	30	90%	92%	F
DSS04.02	Mempertahankan strategi kontinuitas	72	8	80	90%	16	14	30	53%	72%	L
DSS04.03	Kesalahan yang diketahui palsu	75	5	80	94%	13	7	20	65%	79%	L
DSS04.04	Mengatasi dan menutup masalah	29	31	60	48%	16	14	30	53%	51%	P
DSS04.05	Meninjau, memelihara dan meningkatkan rencana berkelanjutan	18	22	40	45%	10	10	20	50%	48%	P
DSS04.06	Melaksanakan pelatihan rencana berkelanjutan	17	13	30	57%	8	8	20	60%	58%	L
DSS04.07	Mengelola pengaturan back-up	50	0	50	100%	1	1	10	90%	95%	F
DSS04.08	Melakukan review ulang	25	15	40	63%	10	10	160	6%	34%	P
Total		**379**	**101**	**480**	**79%**	**113**	**67**	**320**	**35%**	**57%**	**L**

Hasil kuesioner DSS04 Mengelola kontinuitas pada *management practice* 80%, dan *output* hasilnya 34%, dengan skala rata-rata dari *management practice* dan *output* sebesar 54% dengan *rating* L (*Large - Achieved*).

4.8.5 Menghitung Proses dan *Output* DSS05

Pertanyaan yang diajukan kepada responden untuk sub domain DSS05 Mengelola layanan keamanan ke terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-

aktivitas apa saja yang dilakukan pada proses DSS05 yang terdiri dari DSS05.01 , DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06 dan DSS05.07, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Selanjutnya dari pertanyaan-pertanyaan yang disajikan pada kuesioner DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, dan DSS05.07 kemudian dihitung berdasarkan skala *management practice* dan *output* yang dihasilkan pada proses DSS04. Isian kuesioner berisi Ya yang bernilai 1 dan Tidak bernilai 0.

Skala *Management Practice* $\frac{485}{533}$ x 100% = 91%

Skala *Workproduct* $\frac{116}{143}$ x 100% = 81%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS05, mulai dari DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, dan DSS05.07 dapat dilihat pada tabel 4.22

Tabel 4.22 Hasil Pengolahan Data DSS05 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS05.01	Menetapkan kebijakan, tujuan dan ruang lingkup keberlanjutan bisnis	53	7	60	88%	18	2	20	90%	89%	F
DSS05.02	Mengelola konektivitas dan keamanan jaringan	80	10	90	89%	15	5	20	75%	82%	L
DSS05.03	Mengelola keamanan endpoint	85	5	90	94%	9	2	11	82%	88%	F
DSS05.04	Mengelola identitas pengguna (*user identity*) dan akses logis (*logical access*)	113	7	120	94%	18	1	19	95%	94%	F

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS05.05	Mengelola akses fisik ke aset TI	66	4	70	94%	19	1	20	95%	95%	F
DSS05.06	Mengelola dokumen yang sensitif dan perangkat output	44	6	50	88%	19	1	20	95%	92%	F
DSS05.07	Memantau infrastruktur yang berhubungan dengan security events	41	9	50	82%	18	12	30	55%	68%	L
Total		**485**	**42**	**530**	**91%**	**116**	**27**	**140**	**83%**	**87%**	**F**

Hasil kuesioner DSS05 Mengelola layanan keamanan operasional pada *management practice* 91%, dan *output* hasilnya 81%, dengan skala rata-rata dari *management practice* dan *output* sebesar 87% dengan *rating* F (*Fully - Achieved*).

4.8.6 Menghitung Proses dan *Output* DSS06

Pertanyaan yang diajukan kepada responden untuk sub domain DSS06 Mengelola pengendalian proses bisnis terdiri dari pertanyaan-pertanyaan yang menyatakan aktivitas-aktivitas apa saja yang dilakukan pada proses DSS06 terdiri dari DSS06.01 mensejajarkan aktivitas pengendalian yang ada pada proses bisnis dengan sasaran Instansi, DSS06.02 mengendalikan pemrosesan informasi, DSS06.03 mengendalikan pemrosesan informasi, DSS06.04 mengelola *errors* dan *exceptions*, DSS06.05 memastikan keterlacakan peristiwa dan akuntabilitas Informasi dan DSS06.06 mengamankan aset informasi, kemudian untuk melihat *work produt* maka dijawab dengan *output.*

Selanjutnya dari pertanyaan-pertanyaan tersebut diatas kemudian dihitung berdasarkan *management practice* dan *output* yang dihasilkan pada proses DSS06. Isian kuesioner berisi “Ya” yang bernilai 1 dan “Tidak” bernilai 0.

Skala *Management Practice* = $\frac{384}{425}$ x 100% = 90%

Skala *Workproduct* = $\frac{101}{129}$ x 100% = 78%

Berikut ini merupakan hasil pengolahan data kuesioner untuk domain DSS06, mulai dari DSS06.01, DSS06.02, DSS06.03, DSS06.04, DSS06.05 dan DSS06.06, dapat dilihat pada tabel 4.23

Tabel 4.23 Hasil Pengolahan Data DSS06 pada Level 1

Kode	Proses	*Management Practice*				*Output*				Skala (%)	Rating
		Ya	Tidak	Jumlah	%	Ada	Tidak Ada	Jumlah	%		
DSS06.01	Mensejajarkan aktivitas pengendalian yang ada pada proses bisnis dengan sasaran Instansi	76	14	90	84%	15	5	20	75%	80%	L
DSS06.02	Mengendalikan pemrosesan informasi	120	10	130	92%	15	15	30	50%	71%	L
DSS06.03	Mengelola peran, tanggung jawab, hak akses, dan tingkat otoritas	66	4	68	97%	28	1	30	97%	97%	F
DSS06.04	Mengelola errors dan exceptions	43	7	50	86%	18	2	20	90%	88%	F
DSS06.05	Memastikan keterlacakan peristiwa dan akuntabilitas Informasi	29	7	36	81%	16	4	20	80%	80%	L
DSS06.06	Mengamankan aset informasi	50	1	51	98%	9	1	10	90%	94%	F
Total		**384**	**43**	**425**	**90%**	**101**	**28**	**130**	**78%**	**86%**	**F**

Hasil kuesioner DSS06 Mengelola pengendalian proses bisnis pada *management practice* 90%, dan *output* hasilnya 78%, dengan skala rata-rata dari *management practice* dan *output* sebesar 86% dengan *rating* F (*Fully - Achieved*).

4.9 Penilaian *Capability Level*

Pada tahap ini melakukan penilaian *capability level* pada masing-masing proses di DSS01, DSS02, DSS03, DSS04, DSS05 dan DSS06. Proses penentuan *capability* yaitu sebagai berikut :

4.9.1 *Capability Level* proses DSS01

Tabel 4.24 Pemetaan hasil perhitungan kuesioner DSS01 terhadap *capability level* 1

DSS01	**Melaksanakan prosedur operasional**						
	Tujuan	Memberikan hasil layanan operasional TI sesuai rencana.					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 ***Incomplete***	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 ***Performed***	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai Keseluruhan**				F
		DSS01.01	Y				F
		DSS01.02	Y				F
		DSS01.03	Y				F
		DSS01.04	Y				F
		DSS01.05	Y				F

Seperti yang terlihat pada tabel 4.61 diatas *capability level* yang diraih pada proses DSS di level 1 adalah F (*Fully Achieved*).

Karena hasil *capability level* 1 DSS01 Fully. Maka, penulis akan melanjutkan ke level 2. Berikut ini penilaian *capability level* pada level 2 dari proses DSS01 (*Manage Operation*) yang terlihat pada tabel 4.25

Tabel 4.25 *Capability Level* pada proses DSS01 level 2

	Level 0 (%)	**Level 1 (%)**	**Level 2 (%)**		**Level 3 (%)**		**Level 4 (%)**		**Level 5 (%)**	
DSS01		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rata-rata		**92.75**	**93.33**	**85.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

	Level 0 (%)	Level 1 (%)	Level 2 (%)		Level 3 (%)		Level 4 (%)		Level 5 (%)	
DSS01		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Kriteria Rating Pencapaian		**F**	**F**	**F**	**N**	**N**	**N**	**N**	**N**	**N**
Capability Level		**1**	**2**	**2**						

Nilai *Capability Level* pada level 2 yaitu PA 2.1 adalah F (*Fully Achieved*) dan PA 2.2 adalah F (*Fully Achieved*), maka nilai *capability level* 2 untuk DSS01 adalah F. Maka, penilaian akan dilanjutkan ke level 3. Sesuai dengan tabel 4.26

Tabel 4.26 *Capability Level* pada proses DSS01 level 3

	Level 0 (%)	Level 1 (%)	Level 2 (%)		Level 3 (%)		Level 4 (%)		Level 5 (%)	
DSS01		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**92.75**	**93.33**	**85.00**	**82.00**	**65.00**	**00.00**	**0.00**	**0.00**	**0.00**
Kriteria Rating Pencapaian		**F**	**F**	**F**	**L**	**L**	**N**	**N**	**N**	**N**
Capability Level		**1**	**2**	**2**	**3**	**3**	**0**	**0**	**0**	**0**

Hasil *capabilityl* pada level 3 skala atribut proses PA 3.1 bernilai L dan skala atribut proses PA 3.2 bernilai L, maka nilai *capability* pada level 3 adalah L, maka penilaian berhenti di level 3. Proses DSS01 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 2. Level 2 yaitu F (*Fully Achieved*) artinya Pengadilan Militer II-09 Bandung telah menerapkan pengelolaan operasional secara terencana dan termonitor dan telah menerapkan sebagian standar operasional prosedur (SOP) terkait pemeliharaan infrastruktur TI pengelolaan lingkungan dan fasilitas layanan.

4.9.2 *Capability Level* proses DSS02

Tabel 4.27 Pemetaan hasil perhitungan kuesioner DSS02 terhadap *capability level* 1

DSS02	**Mengelola permintaan dan insiden layanan**						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan permintaan dan layanan insiden TI					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**

DSS02	Mengelola permintaan dan insiden layanan						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan permintaan dan layanan insiden TI					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 Incomplete	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 Performed	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai keseluruhan**				F
		DSS02.01	Y				F
		DSS02.02	Y			L	
		DSS02.03	Y				F
		DSS02.04	Y				F
		DSS02.05	Y				F
		DSS02.06					F
		DSS02.07					F

Seperti yang terlihat pada tabel 4.65 diatas *capability level* nilai yang diraih pada proses DSS di level 1 adalah F (*Fully Achieved*). Selanjutnya, penulis akan melanjutkan penilaian ke level 2. Berikut ini merupakan *capability level* pada level 2 dari proses DSS02 (*Manage Service and Incidents*) yang terlihat pada tabel 4.28

Tabel 4.28 *Capability Level* pada proses DSS02 level 2

	Level 0 (%)	**Level 1 (%)**	**Level 2 (%)**		**Level 3 (%)**		**Level 4 (%)**		**Level 5 (%)**	
DSS02		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**90.51**	**80.00**	**65.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Nilai		**F**	**L**	**L**	**N**	**N**	**N**	**N**	**N**	**N**
Kapabilitas		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**

Nilai *Capability Level* pada level 2 yaitu PA 2.1 adalah L (*Largerly Achieved*) dan PA 2.2 adalah L (*Largely Achieved*), maka nilai *capability level* untuk DSS01 adalah L. Nilai *capability* DSS02 pada level 2 adalah L (*Largely achieved*) maka penilaian berhenti di level 1. Karena nilai *capability level* 2 lebih kecil daripada nilai *capability level* 1, maka

penilaian *capability level* berhenti pada level 1. Artinya DSS02 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 1. Level 1 yaitu F (*Fully Achieved*) artinya Pengadilan Militer II-09 Bandung telah proses pengelolaan permintaan dan layanan insiden telah terdefinisi, terdiagnosa, dan mengatasi dan memulihkan insiden.

4.9.3 *Capability Level* proses DSS03

Tabel 4.29 Pemetaan hasil perhitungan kuesioner DSS03 terhadap *capability level* 1

DSS03	**Mengelola masalah**						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan masalah					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 Incomplete	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 Performed	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai keseluruhan**				F
		DSS03.01	Y			L	
		DSS03.02	Y				F
		DSS03.03	Y				F
		DSS03.04	Y				F
		DSS03.05	Y				F

Seperti yang terlihat pada tabel 4.29 *capability level* yang diraih pada proses DSS di level 1 adalah F (*Fully Ahcieved*). Maka, penulis akan melanjutkan ke level 2. Berikut ini merupakan *capability level* pada level 2 dari proses DSS03 (*Mengelola Masalah*) yang terlihat pada tabel 4.30

Tabel 4.30 *Capability Level* pada proses DSS03 level 2

	Level 0 (%)	**Level 1 (%)**	**Level 2 (%)**		**Level 3 (%)**		**Level 4 (%)**		**Level 5 (%)**	
DSS03		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**89.72**	**93.33**	**90.00**	**00.00**	**00.00**	**0.00**	**0.00**	**0.00**	**0.00**
Nilai		**F**	**F**	**F**	**P**	**F**	**N**	**N**	**N**	**N**
Kapabilitas		**1**	**2**	**2**	**3**	**3**	**0**	**0**	**0**	**0**

Nilai *Capability Level* pada level 2 yaitu PA 2.1 adalah F (*Fully Achieved*) dan PA 2.2 adalah F (*Fully Achieved*), maka nilai *capability level* untuk DSS03 level 2 adalah F. Selanjutnya, penilaian akan dilanjutkan ke level 3. Sesuai dengan tabel 4.70

Tabel 4.31 *Capability Level* pada proses DSS03 level 3

	Level 0 (%)	Level 1 (%)	Level 2 (%)		Level 3 (%)		Level 4 (%)		Level 5 (%)	
DSS03		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**89.72**	**93.33**	**90.00**	**46.00**	**97.67**	**0.00**	**0.00**	**0.00**	**0.00**
Nilai		**F**	**F**	**F**	**P**	**F**	**N**	**N**	**N**	**N**
Kapabilitas		**1**	**2**	**2**	**3**	**3**	**0**	**0**	**0**	**0**

Hasil penilaian *capability level* untuk level 3 adalah skala atribut proses PA 3.1 bernilai P dan skala atribut PA 3.2 bernilai F, nilai *capability* DSS03 pada level 3 adalah P (*Particially achieved*) maka penilaian berhenti di level 3. Maka DSS03 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 2. Level 2 yaitu F (*Fullly Achieved*) artinya Pengadilan Militer II-09 Bandung telah mengelola manajemen pengelolaan masalah.

4.9.4 *Capability Level* proses DSS04

Berikut ini akan dilakukan penentun dan penilaian terhadap *capability* proses yang dirancang pada penelitian ini. Penilaian dimulai dari level 1.

Tabel 4.32 Pemetaan hasil perhitungan kuesioner DSS04 terhadap *capability level* 1

DSS04	**Mengelola kontinuitas**						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan kontinuitas					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 Incomplete	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 Performed	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai keseluruhan**			L	

DSS04	Mengelola kontinuitas						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan kontinuitas					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
		DSS04.01	Y				F
		DSS04.02	Y			L	
		DSS04.03	Y			L	
		DSS04.04	Y		P		
		DSS04.05	Y		P		
		DSS04.06				L	
		DSS04.07				F	
		DSS04.08			P		

Seperti yang terlihat pada tabel 4.32 *capability level* yang diraih pada proses DSS di level 1 adalah L (*Largely Achieved*). Selanjutnya penilaian berhenti di level 1 karena nilai *capability level* tidak mencapai *Fully Achieved,* maka proses DSS04 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 0. Level 0 yaitu Pengadilan Militer II-09 Bandung belum melakukan pengelolaan TI terkait manajemen kontinuitas.

4.9.5 C*apability Level* proses DSS05

Tabel 4.33 Pemetaan hasil perhitungan kuesioner DSS05 terhadap *capability level* 1

DSS05	Mengelola layanan keamanan						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan kontinuitas					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 Incomplete	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 Performed	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai keseluruhan**			L	
		DSS05.01	Y				F
		DSS05.02	Y			L	

DSS05	Mengelola layanan keamanan						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan kontinuitas					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
		DSS05.03	Y				F
		DSS05.04	Y				F
		DSS05.05	Y				F
		DSS05.06	Y				F
		DSS05.07	Y			L	

Seperti yang terlihat pada tabel 4.33 *capability level* yang diraih pada proses DSS di level 1 adalah F (*Fully Achieved*). Kemudian hasil *capability level* 1 DSS05 adalah L. Maka, penulis akan melanjutkan ke level 2. Berikut ini merupakan *capability level* pada level 2 dari proses DSS05 (Mengelola layanan keamanan) yang terlihat pada tabel 4.34

Tabel 4.34 *Capability Level* pada proses DSS05 level 2

	Level 0 (%)	**Level 1 (%)**	**Level 2 (%)**		**Level 3 (%)**		**Level 4 (%)**		**Level 5 (%)**	
DSS05		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**85.97**	**91.67**	**87.50**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Nilai		**F**	**F**	**F**	**N**	**N**	**N**	**N**	**N**	**N**
Kapabilitas		**1**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**

Nilai *Capability Level* pada level 2 yaitu PA 2.1 adalah F (*Fully Achieved*) dan PA 2.2 adalah F (*Fully Achieved*), maka nilai *capability level* 2 adalah F. Maka, penilaian akan dilanjutkan ke level 3. Sesuai dengan tabel 4.35

Tabel 4.35 *Capability Level* pada proses DSS05 level 3

	Level 0 (%)	**Level 1 (%)**	**Level 2 (%)**		**Level 3 (%)**		**Level 4 (%)**		**Level 5 (%)**	
DSS05		**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**	**PA**
		1.1	**2.1**	**2.2**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**	**5.2**
Rerata		**85.97**	**91.67**	**87.50**	**78.00**	**88.00**	**0.00**	**0.00**	**0.00**	**0.00**
Nilai		**F**	**F**	**F**	**L**	**F**	**N**	**N**	**N**	**N**
Kapabilitas		**1**	**2**	**2**	**3**	**3**	**0**	**0**	**0**	**0**

Hasil *capability* pada level 3 skala atribut proses PA 3.1 bernilai L dan skala atribut proses PA 3.2 bernilai F, maka nilai *capability* pada level 3 adalah L, maka penilaian berhenti di level 3. Proses DSS05 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 2. Level 2 yaitu F (*Fully Achieved*) artinya Pengadilan Militer II-09 Bandung telah menerapkan dan mengelola manajemen pengelolaan layanan keamanan.

4.9.6 C*apability Level* proses DSS06

Tabel 4.36 Pemetaan hasil perhitungan kuesioner DSS06 terhadap *capability level* 1

DSS06	**Mengelola kendala proses bisnis**						
	Tujuan	Menyediakan pendekatan manajemen pengelolaan kontinuitas					
	Menilai Hasil Pencapaian	**Kriteria**	**pakah Kriteria Terpenuhi? Y/N**	**N**	**P**	**L**	**F**
Level 0 Incomplete	**Pada level ini tidak ada bukti dalam pencapaian tujuan proses.**	Pada level ini tidak ada bukti dalam pencapaian tujuan proses.	Y				F
Level 1 Performed	**PA 1.1 Proses yang diimplementasikan mencapai tujuan prosesnya.**	Hasil dari proses yang sedang dicapai:	**Nilai keseluruhan**			F	
		DSS05.01	Y			L	
		DSS05.02	Y			L	
		DSS05.03	Y				F
		DSS05.04	Y				F
		DSS05.05	Y			L	
		DSS05.06	Y				F

Seperti yang terlihat pada tabel 4.36 *capability level* yang diraih pada proses DSS di level 1 adalah L (*Large Achieved*). Selanjutnya penilaian akan dilanjutkan ke level 2. Berikut ini merupakan *capability level* pada level 2 dari proses DSS06 (Mengelola layanan keamanan) yang terlihat pada tabel 4.37

Tabel 4.37 *Capability Level* pada proses DSS06 level 2

	Level 0 (%)	Level 1 (%)	Level 2 (%)		Level 3 (%)		Level 4 (%)		Level 5 (%)	
DSS06		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rerata		88.18	91.67	85.00	0.00	0.00	0.00	0.00	0.00	0.00
Nilai		F	F	F	N	N	N	N	N	N
Kapabilitas		1	2	2	0	0	0	0	0	0

Nilai *Capability Level* pada level 2 yaitu PA 2.1 adalah F (*Fully Achieved*) dan PA 2.2 adalah F (*Fully Achieved*), maka nilai *capability level* untuk DSS06 adalah F. Maka, penilaian akan dilanjutkan ke level 3. Sesuai dengan tabel 4.38

Tabel 4.38 *Capability Level* pada proses DSS06 level 3

	Level 0 (%)	Level 1 (%)	Level 2 (%)		Level 3 (%)		Level 4 (%)		Level 5 (%)	
DSS06		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rerata		88.18	91.67	85.00	36.00	68.33	0.00	0.00	0.00	0.00
Nilai		F	F	F	P	L	N	N	N	N
Kapabilitas		1	2	2	3	3	0	0	0	0

Hasil penilaian *capability level* untuk level 3 adalah skala atribut proses PA 3.1 bernilai P dan skala atribut PA 3.2 bernilai L, nilai *capability* DSS06 pada level 3 adalah P (*Particially achieved*) maka penilaian berhenti di level 3. Maka DSS05 Pengadilan Militer II-09 Bandung saat ini berada pada *capability level* 2. Level 2 yaitu F (*Fully Achieved*) artinya Pengadilan Militer II-09 Bandung telah menerapkan mengelola manajemen pengelolaan pengendalian proses bisnis.

4.10 Analisis GAP

Berdasarkan perhitungan *capability level* dan evaluasi yang diakukan pada penelitian ini analisis GAP untuk seluruh proses pada domain DSS, yaitu proses DSS01, DSS02, DSS03, DSS04, DSS04, DSS05, dan DSS06, yang dapat dilihat pada tabel 4.39

Tabel 4.39 Analisis GAP proses DSS

No	Nama Proses	Level Saat Ini	Level Target	GAP
1	DSS01 Mengelola Operasional	2	3	1
2	DSS02 Mengelola Permintaan	1	3	2

No	Nama Proses	Level Saat Ini	Level Target	GAP
	dan Insiden Layanan			
3	DSS03 Mengelola Masalah	2	3	1
4	DSS04 Mengelola Kontinuitas	0	3	3
5	DSS05 Mengelola Layanan Keamanan	2	3	1
6	DSS06 Mengelola Pengendalian Proses Bisnis	2	3	1

4.11 Pengumpulan Bukti dan Kondisi *Existing*

Pada penelitian mengenai audit ini dilakukan pengumpulan bukti berdasarkan standar COBIT 5 dan kondisi saat ini yang terdapat di Pengadilan Militer II-09 Bandung pada Sistem Informasi Penelusuran Perkara di domain DSS (*Deliver, Service and Support*). Berikut adalah hasil pengumpulan bukti, berupa observasi, wawancara dan kuesioner.

Tabel 4.40 Pengumpulan Bukti Proses DSS01

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS01 Melaksanakan prosedur operasional	Jadwal Operasional	Dokumen terkait Jadwal Operasional	Ada	Piket 24 jam.
	Backup log	Rekaman aktivitas	Ada	Rekaman CCTV, laporan piket per 24 jam
DSS02 Mengelola layanan TI *outsourcing*	Rencana Jaminan Independen	Dokumen rencana jaminan independent dengan TI *outsourcing*	Ada	Kontrak/SLA (*Service Level Agreement*) dengan pihak *Outsourcing*
DSS01.03 Mengelola infrastruktur TI	Aturan *monitoring aset* dan *event log*	Dokumen monitoring dan pengawasan terhadap asset dan insiden	Ada	Laporan SIMAK BMN
	Event log	Rekaman dari kegiatan	Ada	Rekaman CCTV
	Incident tickets	Dokumen terkait insiden	Ada	Formulir Penanganan *Hardware/*Data Rusak.
DSS01.04 Mengelola lingkungan	Kebijakan lingkungan kerja	Dokumen mengenai kebijakan	Tidak Ada	-

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
		lingkungan		
	Laporan polis asuransi	Dokumen yang berisi mengenai kebijakan asuransi	Ada	Jika ada perawatan terkait infrastruktur TI atau Sistem Informasi, Aplikasi, hanya ada garansi yang berjangka tertentu setelah pembelian, tetapi jika ada kerusakan atau perawatan maka diperbaiki oleh pihak ketiga dengan kontrak atau penunjukan langsung.
DSS01.05 Mengelola fasilitas-fasilitas	Laporan penilaian fasilitas	Dokumen mengenai penilaian fasilitas	Ada	Dokumen Laporan SIMAK BMN, jika ada fasilitas yang berupa asset dan harus dimusnahkan, maka secara independent akan dilakukan penilaian oleh pihak ketiga yaitu KPKNL.
	Kesadaran kesehatan dan keselamatan	Daftar mengenai kesehatan atau keselamatan	Ada	Keamanan oleh *security*

Tabel 4.41 Pengumpulan Bukti Proses DSS02

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS02.01 Mendefinisikan Skema Klasifikasi Insiden dan Permintaan Layanan	Skema dan model klasifikasi permintaan insiden dan layanan	Skema dan model klasifikasi permintaan insiden dan layanan	Tidak Ada	-
	Aturan untuk tindak lanjut	Aturan mengenai	Ada	Formulir insiden

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
	insiden	insiden terkait urgensi		
	Kriteria untuk pendaftaran masalah	Kriteria masalah	Ada	Formulir insiden
DSS02.02 Merekam, mengklasifikasikan, dan memprioritaskan permintaan dan insiden	Log insiden dan permintaan layanan	Rekaman permintaan layanan	Tidak Ada	-
	Insiden dan permintaan layanan yang diklasifikasikan dan diprioritaskan	Dokumen insiden dan permintaan layanan yang diklasifikasikan dan diprioritaskan	Ada	Formulir insiden
DSS02.03 Memverifikasi, menyetujui dan memenuhi permintaan	Permintaan layanan yang disetujui	Dokumen permintaan layanan yang disetujui	Ada	Formulir Penanganan *Hardware*/Data Rusak.
	Permintaan layanan terpenuhi	Dokumen permintaan layanan yang telah terpenuhi	Ada	Formulir Penanganan *Hardware*/Data Rusak.
DSS02.04 Menyelidiki, mendiagnosa dan mengalokasikan insiden	Gejala insiden	Daftar gejala insiden	Ada	Formulir insiden
	Log masalah	Rekaman masalah	Ada	Formulir insiden
DSS02.05 Menyelesaikan dan memulihkan insiden	Resolusi insiden	Daftar solusi insiden	Ada	Kontrak dengan Pihak Ketiga mengenai penanganan insiden
DSS02.06 Menyelesaikan dan memulihkan insiden	Permintaan layanan dan insiden ditutup	Dokumen permintaan layanan dan insiden ditutup	Tidak Ada	-
	Konfirmasi pengguna atas pemenuhan atau resolusi yang memuaskan	Konfirmasi pengguna atas pemenuhan atau resolusi layanan insiden	Tidak Ada	-
DSS02.07 Melacak status dan membuat laporan	Status insiden dan laporan tren	Laporan status insiden dan laporan tren	Ada	Laporan Hakim Pengawas Perencanaan, TI dan Pelaporan
	Laporan permintaan status pemenuhan dan tren	Laporan permintaan status pemenuhan dan tren	Ada	Laporan Hakim Pengawas Perencanaan, TI dan Pelaporan

Tabel 4.42 Pengumpulan Bukti Proses DSS03

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS03.01 Mengidentifikasi dan mengklasifikasikan masalah	Skema klasifikasi masalah	Skema dan model klasifikasi masalah	Tidak Ada	-
	Laporan status masalah	Laporan status masalah	Ada	Formulir permasalahan
	Pendaftaran masalah	Daftar permasalahan	Ada	Formulir permasalahan
DSS03.02 Mengivestigasi dan mendiagnosis masalah	Akar penyebab masalah	Laporan akar penyebab masalah	Tidak Ada	-
	Laporan resolusi masalah	Laporan berupa resolusi masalah	Ada	Laporan Permasalahan
DSS03.03 Kesalahan yang diketahui palsu	Catatan kesalahan yang dikenal	Laporan kesalahan yang terdeteksi	Ada	Laporan Permasalahan
	Solusi yang diusulkan untuk kesalahan yang diketahui	Laporan solusi	Ada	Laporan Permasalahan
DSS03.04 Mengatasi dan menutup masalah	Catatan masalah yang ditutup	Daftar catatan masalah yang ditutup	Ada	Laporan Permasalahan
	Komunikasi pengetahuan yang dipelajari	Komunikasi terhadap masalah dan cara penanganannya	Ada	Laporan Permasalahan
DSS03.05 Menjalankan manajemen masalah secara proaktif	Laporan monitoring resolusi masalah	Laporan monitoring resolusi masalah	Ada	Laporan Permasalahan
	Solusi berkelanjutan yang teridentifikasi	Laporan solusi berkelanjutan yang teridentifikasi	Ada	Laporan Permasalahan

Tabel 4.43 Pengumpulan Bukti Proses DSS04

Sub Proses	Analisis dampak bisnis	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS04.01 Menetapkan kebijakan, tujuan dan ruang lingkup keberlanjutan bisnis	Kebijakan dan tujuan untuk kelangsungan bisnis	Kebijakan dan tujuan untuk kelangsungan bisnis	Tidak Ada	
	Skenario insiden yang mengganggu	Skenario insiden yang mengganggu	Tidak Ada	

Sub Proses	Analisis dampak bisnis	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
	Penilaian kemampuan kesinambungan saat ini dengan kesenjangan	Penilaian kemampuan kesinambungan saat ini dengan kesenjangan	Tidak Ada	
DSS04.02 Mempertahankan strategi kontinuitas	Analisis dampak bisnis	Analisis dampak bisnis	Tidak Ada	
	Persyaratan kontinuitas	Persyaratan kontinuitas	Tidak Ada	
	Opsi strategis yang disetujui	Opsi strategis yang disetujui	Tidak Ada	
DSS04.03 Kesalahan yang diketahui palsu	Tindakan dan komunikasi respons insiden	Tindakan dan komunikasi respons insiden	Tidak Ada	
	BCP (rencana bisnis kesinambungan)	BCP (rencana bisnis kesinambungan)	Tidak Ada	
DSS04.04 Mengatasi dan menutup masalah	Tujuan Tes	Tujuan Tes	Tidak Ada	
	Tujuan Latihan	Tujuan Latihan	Tidak Ada	
	Hasil dan rekomendasi tes	Hasil dan rekomendasi tes	Tidak Ada	
DSS04.05 Meninjau, memelihara dan meningkatkan rencana berkelanjutan	Persyaratan Pelatihan	Persyaratan Pelatihan	Tidak Ada	
	Rekomendasi perubahan pada rencana	Rekomendasi perubahan pada rencana	Tidak Ada	
DSS04.06 Melaksanakan pelatihan rencana berkelanjutan	Training requirements	Training requirements	Tidak Ada	
	Memantau hasil keterampilan dan kompetensi	Memantau hasil keterampilan dan kompetensi	Tidak Ada	-
DSS04.07 Mengelola pengaturan back-up	Hasil tes backup data	Hasil tes backup data	Ada	*Backup Data* Sistem Informasi Penelusuran Perkara
DSS04.08 Melakukan review ulang	*Post-resumption review report*	*Post-resumption review report*	Tidak Ada	
	Perubahan yang disetujui pada rencana	Perubahan yang disetujui pada rencana	Tidak Ada	

Tabel 4.44 Pengumpulan Bukti Proses DSS05

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS05.01 Menetapkan kebijakan, tujuan dan ruang lingkup keberlanjutan	Kebijakan pencegahan perangkat lunak berbahaya	Kebijakan pencegahan perangkat lunak berbahaya	Ada	Program Kerja di RKAKL dan antivirus legal telah terinstal di semua

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
bisnis				computer *user*
	Evaluasi potensi ancaman	Evaluasi potensi ancaman	Ada	Dilakukan *update* antivirus per bulan
DSS05.02 Mengelola konektivitas dan keamanan jaringan	Kebijakan keamanan konektivitas	Kebijakan keamanan konektivitas	Ada	Dibatasi oleh *firewall*
	Hasil tes penetrasi	Hasil tes penetrasi	Tidak ada	-
DSS05.03 Mengelola keamanan endpoint	Kebijakan keamanan untuk perangkat endpoint	Kebijakan keamanan untuk perangkat endpoint	Ada	Menggunakan *Antivirus*
DSS05.04 Mengelola identitas pengguna (user identity) dan akses logis (*logical access*)	Hak akses pengguna yang disetujui	Hak akses pengguna yang disetujui	Ada	Pengelolaan hak akses
	Hasil review akun user dan hak istimewa	Hasil review akun user dan hak istimewa	Ada	Pengelolaan hak akses
DSS05.05 Mengelola akses fisik ke aset TI	Permintaan akses yang disetujui	Permintaan akses yang disetujui	Ada	Pengelolaan hak akses
	Log akses	Log akses	Ada	Pengelolaan hak akses
DSS05.06 Mengelola dokumen yang sensitif dan perangkat output	Inventarisasi dokumen dan perangkat sensitive	Inventarisasi dokumen dan perangkat sensitif	Ada	Akses ke perangkat menggunakan *password* atau *finger scanning*
	Access privileges (hak akses istimewa)	Access privileges (hak akses istimewa)	Ada	Akses ke perangkat menggunakan *password* atau *finger scanning*
DSS05.07 Memantau infrastruktur yang berhubungan dengan security events	Keamanan event logs	Keamanan event logs	Ada	*Review*
	Karakteristik insiden keamanan	Karakteristik insiden keamanan	Ada	*Firewall*
	Keamanan incidents ticket	Keamanan incidents ticket	Tidak Ada	-

Tabel 4.45 Pengumpulan Bukti Proses DSS06

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
DSS06.01	Hasil tinjauan	Hasil tinjauan	Ada	Daftar di

Sub Proses	*Output/Bukti*	Deskripsi	Keberadaan *output* (Ada/Tidak)	Keterangan
Mensejajarkan aktivitas pengendalian yang ada pada proses bisnis dengan sasaran Instansi	efektivitas pemrosesan	efektivitas pemrosesan		Bagian Umum dan Keuangan
	Analisis akar penyebab dan rekomendasi	Analisis akar penyebab dan rekomendasi	Ada	Daftar di Bagian Umum dan Keuangan
DSS06.02 Mengendalikan pemrosesan informasi	Memproses laporan pengendalian	Memproses laporan pengendalian	Tidak Ada	-
	Persyaratan kontinuitas	Persyaratan kontinuitas	Ada	SAKIP
	Opsi strategis yang disetujui	Opsi strategis yang disetujui	Ada	Disposisi
DSS06.03 Mengelola peran, tanggung jawab, hak akses, dan tingkat otoritas	Peran dan tanggung jawab yang dialokasikan	Peran dan tanggung jawab yang dialokasikan	Ada	Daftar Personil
	Tingkat kewenangan yang dialokasikan	Tingkat kewenangan yang dialokasikan	Ada	Daftar Personil
	Hak akses yang dialokasikan	Hak akses yang dialokasikan	Ada	Daftar Personil
DSS06.04 Mengelola errors dan exceptions	Bukti koreksi kesalahan dan remediasi	Bukti koreksi kesalahan dan remediasi	Tidak Ada	-
	Laporan kesalahan dan analisis akar penyebab	Laporan kesalahan dan analisis akar penyebab	Ada	Formulir Insiden
DSS06.05 Memastikan keterlacakan peristiwa dan akuntabilitas Informasi	Persyaratan penyimpanan	Persyaratan penyimpanan	Ada	Bagian Perencanan, TI dan Pelaporan
	Catatan Transaksi	Catatan Transaksi	Ada	Audit Trail
DS DSS06.06 Mengamankan aset informasi	Laporan pelanggaran	Laporan pelanggaran	Tidak Ada	-

4.12 Rekomendasi

Rekomendasi diberikan berdasarkan panduan COBIT 5 dan ITIL V3 2011, yaitu sebagai berikut :

1. Rekomendasi DSS01

   Berdasarkan hasil analisis GAP dan pengumpulan bukti dan terkait dengan kondisi saat ini di Pengadilan Militer II-09 Bandung yang berada pada level 2 pada tingkat

Managed Process dan target pada level 3 pada tingkat *Established Process*, maka untuk meningkatkan kualitas pelayanan operasional adalah sebagai berikut :

a. Memberikan pelatihan kepada pegawai di Pengadilan Militer II-09 Bandung dengan memberikan pemahaman tentang menjaga aset yang berupa infrastruktur TI, misalnya berupa membuat *wallpaper* di komputer atau laptop atau *banner* berupa himbauan menjaga computer dan infrastruktur TI.
b. Terkait dengan layanan insiden, Pengadilan Militer II-09 Bandung belum mempunyai *tools* yang membantu melakukan pencatatan insiden dalam penanganan insiden, karena jika ada insiden masih bersifat manual yaitu dengan pencatatan menggunakan blanko/formulir permintaan layanan terkait insiden.
c. ITIL V3 2011 memberikan rekomendasi yaitu :
    1) Menentukan ruang lingkup dan batasan untuk seluruh kegiatan operasional.
    2) Mendefinisikan proses-proses kegiatan operasional yang akan dilaksanakan.
    3) Membuat *service desk / help desk.*

2. Rekomendasi DSS02

Terkait proses DSS02 masih terkait dengan proses DSS01, kondisi saat ini proses DSS02 berada pada level 1 pada tingkat *Performed Process* dan target pada level 3 pada tingkat *Established Process,* maka yang perlu dilakukan adalah :

a. Melakukan perencanaan mengenai cara mengatasi dan memulihkan insiden berdasarkan skala prioritas.
b. Mengidentifikasi permintaan dan layanan insiden berdasarkan klasifikasi dan prioritas.
c. Membuat standar operasional prosedur terkait permintaan dan insiden layanan di Pengadilan Militer II-09 Bandung.
d. Melakukan evaluasi secara periodik minimal 3 bulan sekali mengenai permintaan dan layanan insiden.

e. ITIL V3 2011 merekomendasikan yaitu :

1) Mendefinisikan permintaan dan insiden layanan, berdasarkan kategori/klasifikasi, prioritas dan penyelesaian.

2) Membuat laporan permintaan dan insiden layanan.

3. Rekomendasi DSS03

Terkait proses DSS03 kondisi saat ini proses berada pada level 2 pada tingkat *Managed Process* dan target pada level 3 pada tingkat *Established Process,* maka yang perlu dilakukan adalah :

a. Melakukan pengumpulan data terkait permasalahan yang terjadi.

b. Membuat perencanaan atau kebijakan terkait dengan penanganan masalah, sehingga tidak akan berdampak pada proses bisnis.

c. ITIL memberikan rekomendasi berupa :

1) Menidentifikasi masalah berdasarkan kategori, proritas yang terjadi serta penanganannya.

2) Membuat laporan permasalahan terkait system informasi.

4. Rekomendasi DSS04

Kondisi saat ini proses berada pada level 0 pada tingkat *Incomplete Process* dan target pada level 3 pada tingkat *Established Process,* maka yang perlu dilakukan adalah :

a. Menetukan dan mengembangkan kebijakan keberlangsungan bisnis terkait TI, tujuan dan ruang lingkup.

b. Melakukan evaluasi terkait BCP jika direlasikan ke tujuan bisnis Pengadilan Militer II-09 Bandung.

c. Menambah staf khusus dibagian TI karena jika terdapat personil yang merangkap tupoksi maka tidak akan maksimal dalam melayani permintaan insiden atau masalah layanan.

d. ITIL V3 memberikan rekomendasi berupa :

- Membuat strategi yang berkelanjutan dan mengevaluasi yang hemat biaya dan memastikan terkait pemulihan akibat bencana atau insiden/masalah.

5. Rekomendasi DSS05

   Kondisi saat ini proses berada pada level 2 pada tingkat *Managed Process* dan target pada level 3 pada tingkat *Established Process,* maka yang perlu dilakukan adalah :

   a. Memberikan pemahaman kepada *user* dalam hal hak akses ke perangkat atau ruangan TI yang sangat sensitif milih Pengadilan Mliter II-09 Bandung yang sifatnya rahasia, tidak membolehkan pihak eksternal yang tidak disetujui untuk masuk.
   b. Menerapkan enkripsi informasi pada pertukaran data dan informasi.
   c. Menerapkan laporan penetrasi secara berkala.
   d. ITIL V3 memberikan rekomendasi :
      1) Mendefinisikan proses pengelolaan layanan keamanan data dan informasi.
      2) Membuat dokumentasi terkait potensi ancaman terhadap layanan keamanan data dan informasi.
      3) Mendefinisikan dan menetapkan kemungkinan risiko layanan keamanan data dan informasi dan penanganan risiko tersebut.

6. Rekomendasi DSS06

   Terkait proses DSS06 kondisi saat ini proses berada pada level 2 pada tingkat *manage process* dan target pada level 3 pada tingkat *Established Process,* maka yang perlu dilakukan adalah :

   a. Melakukan inovasi pada proses bisnis di Pengadilan Militer II-09 Bandung.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pada audit Sistem Informasi Penelusuran Perkara yang dilakukan di Pengadilan Militer II-09 Bandung dengan menggunakan COBIT 5 dan ITIL V3 2011.

1. Pengelolaan layanan Sistem Informasi Penelusuran Perkara di Pengadilan Militer II-09 Bandung adalah :
   a. DSS01 berada *capability level* 2, artinya manajemen kinerja proses dan *output* kinerja pengelolaan operasional telah terkelola dengan baik.
   b. DSS02 berada *capability level* 1, artinya permintaan dan layanan insiden telah terdefinisi.
   c. DSS03 berada *capability level* 2, artinya manajemen pengelolaan masalah dan *output* kinerja telah sesuai dan memenuhi harapan.
   d. DSS04 berada *capability level* 0, artinya proses mengelola kontinuitas gagal dalam mencapai tujuan.
   e. DSS05 berada *capability level* 2, artinya manajemen pengelolaan layanan keamanan kinerja proses dan *output* kinerja telah sesuai dan memenuhi harapan dan terkelola dengan baik.
   f. DSS06 berada *capability level* 2, artinya manajemen pengelolaan kendala proses bisnis dan *output* kinerja telah sesuai dan memenuhi harapan dan terkelola dengan baik.
2. Rekomendasi keseluruhan dari seluruh proses adalah :
   a. Mempertahankan aktivitas-aktivitas pada proses yang telah berjalan cukup baik dan melakukan evaluasi jika terdapat kesalahan.
   b. Melakukan inovasi pada proses bisnis menuju Pengadilan Militer II-09 Bandung yang lebih baik.
   c. Pada hasil pengukuran nilai *capability* maka proses yang harus ditingkatkan adalah pada proses DSS0 dan DSS04.

5.2 Saran

Berikut ini adalah saran yang disampaikan untuk penelitian selanjutnya yaitu :

1. Pengukuran penilaian dapat dilakukan dengan memperdalam lagi antara integrasi standar *framework* COBIT 5 dan ITIL V3 2011.
2. Pemilihan metode pengukuran dan perhitungan dilakukan dengan metode yang berbeda.
3. Rekomendasi hasil penelitian dapat dilanjutkan dengan menggunakan analisis kepuasan pengguna berdasarkan analsis SWOT pada ITIL V3 2011 sehingga rekomendasi mempunyai dasar yang kuat.

DAFTAR PUSTAKA

AAIPI. Standar Audit Intern Pemerintah Indonesia. AAIPI, Jakarta. 2013.

Ajismanto, Fahmi. "Analisis Domain Proses COBIT Framework 5 Pada Sistem Informasi Worksheet (Studi Kasus: Perguruan Tinggi STMIK, Politeknik Palcomtech)." Cogito Smart Journal/VOL. 3/NO. 2/DEC 2017 (2017), 207-221.

Bandung, Pengadilan Militer II-09. Jumat Juli 2019. Pengadilan Militer II-09 Bandung. <https://dilmil-bandung.go.id/wp-content/uploads/2017/09/Profil-Pengadilan-Militer-II-09-B andung-2016-OK-BOSS-Compress.pdf>.

—. Reviu Ke-2 Rencana Strategis (Renstra) Pengadilan Militer II-09 Bandung. Bandung. Bandung, Pengadilan Militer II-09 Bandung. 2018.

Effendy, Faried, Dewa, Bahana Sukma , dan Hariyanti, Eva. "Problem Management Teknologi Informasi Berdasarkan Kerangka Kerja ITIL V3 dan COBIT 5." Jurnal Sistem Informasi Bisnis 02 (2018) On-line : http://ejournal.undip.ac.id/index.php/jsinbis (2018), DOI : 10.21456/vol8iss2pp157-165.

Eka Putri, Rahmi. "Penilaian Kapabilitas Proses Tata Kelola TI Berdasarkan Proses." Jurnal CoreIT, Vol.2, No.1, Juni 2016 (2016), 41-54.

Fryonanda, Harfebi, Sokoco, Heru dan Nurhadryani, Yani. "Evaluasi Infrastruktur Teknologi Informasi dengan COBIT 5 dan ITIL V3." *).* JUTI: Jurnal Ilmiah Teknologi Informasi - Volume 17, Nomor 1, Januari 2019, 1 – 11 (2019).

Hanuma, Soraya dan Kiswara, Endang. "Analisis Balanced Scorecard Sebagai Alat Ukur Kinerja Perusahaan (Studi Kasus pada PT Astra Honda Motor)." (2011).

ISACA. *A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, ISACA. 2012.

—. Cobit 5 ISACA's new framework for IT Governance, Risk, Security and Auditing. ISACA. n.d.

—. Enabling Processes. Rolling Meadows: ISACA. 2012.

—. Information Systems Auditing *:* Tools and Techniques--Creating Audit Programs. Rolling Meadows, ISACA. 2016.

—. Process Assesment Model (PAM): Using COBIT 5. Rolling Meadows, ISACA. 2013.

ITIL. ITIL Service Operation. Norwich, TSO. 2011.

Kaban, Ita Ernala. "Tata Kelola Teknologi Informasi (IT Governance)." (n.d.).

Kagermann, Henning, dkk. Internal Audit Handbook, Management with the SAP - Audit Roadmap. Springer, Verlag Berlin Heidelberg. 2008.

Mulyanto, Agus. Sistem Informasi Konsep dan Aplikasi. Pustaka Pelajar, Yogyakarta. 2009.

Romney, Masrhall B dan Steinbart, Paul John. Thirteenth Edition Accounting Informatiopn Systems. New Jersey: Pearson Education, 2015.

Sandra, Senft, Gallegos, Frederik, dan Davis, Aleksandra. Information Technology Control and Audit Fourth Edition. Boca Raton, Taylor & Francis Group. 2013.

Saputro, Fachruddin Edi Nugroho, Utami, Ema dan Al Fatta, Hanif. "Integrasi Framework COBIT 5 dan ITIL V.3 Untuk Membangun Model Tata Kelola Infrastruktur Teknologi Informasi." Konferensi Nasional Sistem Informasi 2018, STMIK Atma Luhur Pangkalpinang, 8 – 9 Maret 2018 (2018).

Soejono, Karni. "Audit Khusus dan Audit Forensik : Tantangan dan Peluang Auditor Independen." Ekuitas Vol.2, No.1 Maret 1998 : 36-50 (n.d.).

Susanto, Azhar. Sistem Informasi Akuntansi. Lingga Jaya, Bandung. 2013.

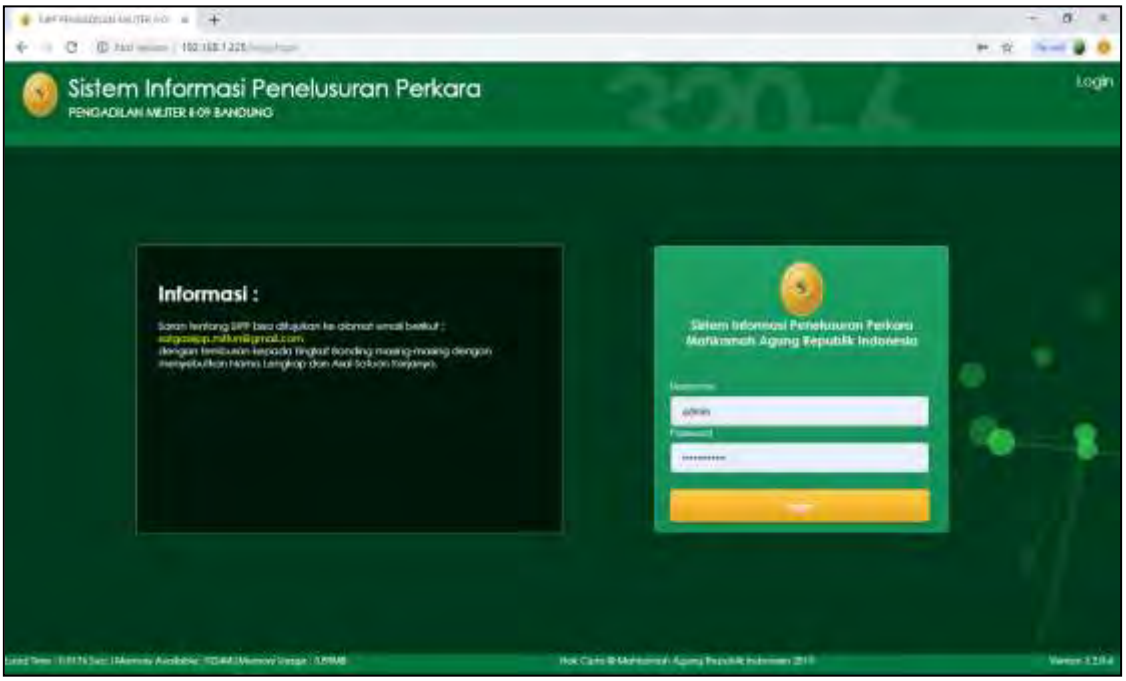
Sutarman. Pengantar Teknologi Informasi. Bumi Aksara, Jakarta. 2009.

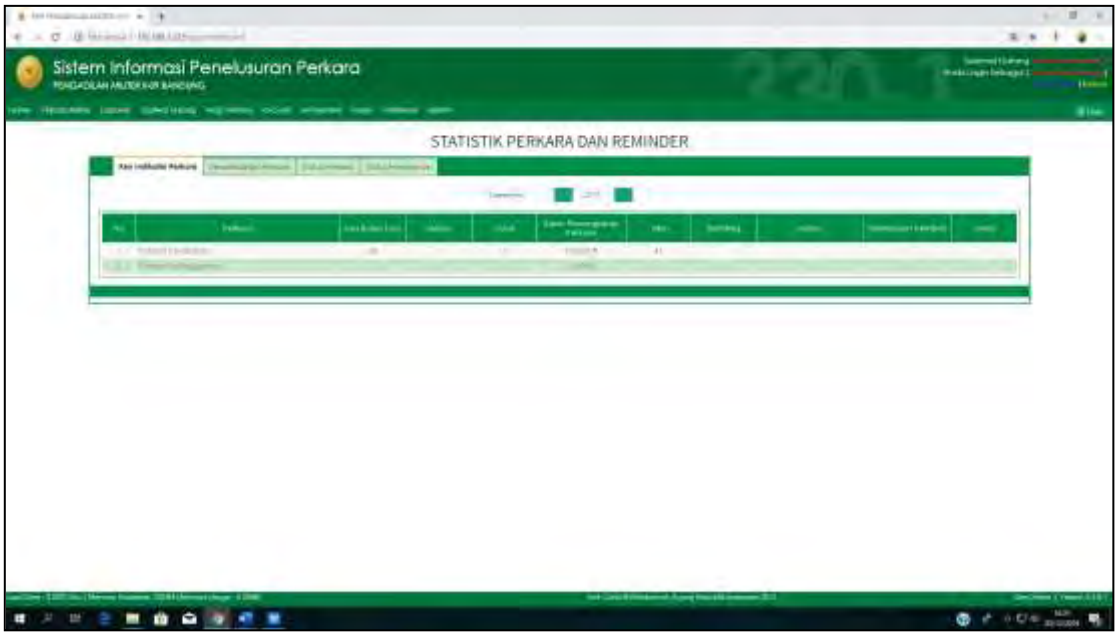
UK, ITSMF. An Introduction Overview of ITIL 2011. Norwich, TSO. 2012.

Wibowo, Aldi Satriani, Selo, dan Adipta, Dani. "Kombinasi Framework COBIT 5, ITIL dan ISO/IEC 27002 untuk membangun Tata Kelola Teknologi Informasi di Perguruan Tinggi." Seminar Nasional Teknologi Informasi dan Komunikasi 2016 (SENTIKA 2016), Yogyakarta, 18-19 Maret 2016 (ISSN: 2089-9815) (2016).

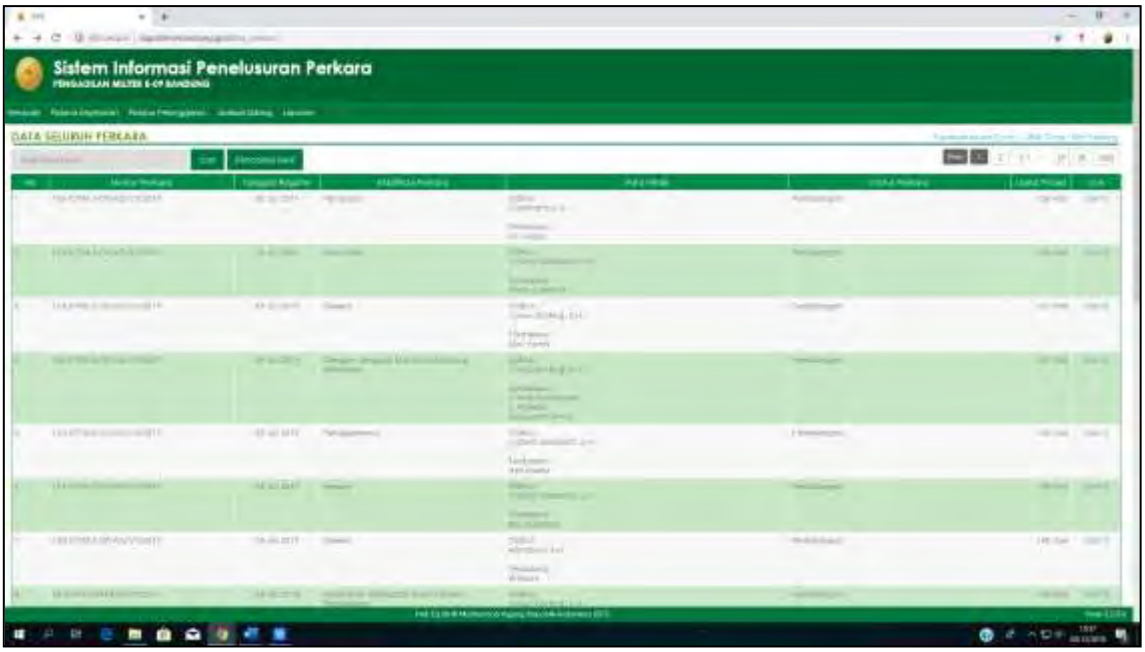
LAMPIRAN

Sistem Informasi Penelusuran Perkara Server Lokal

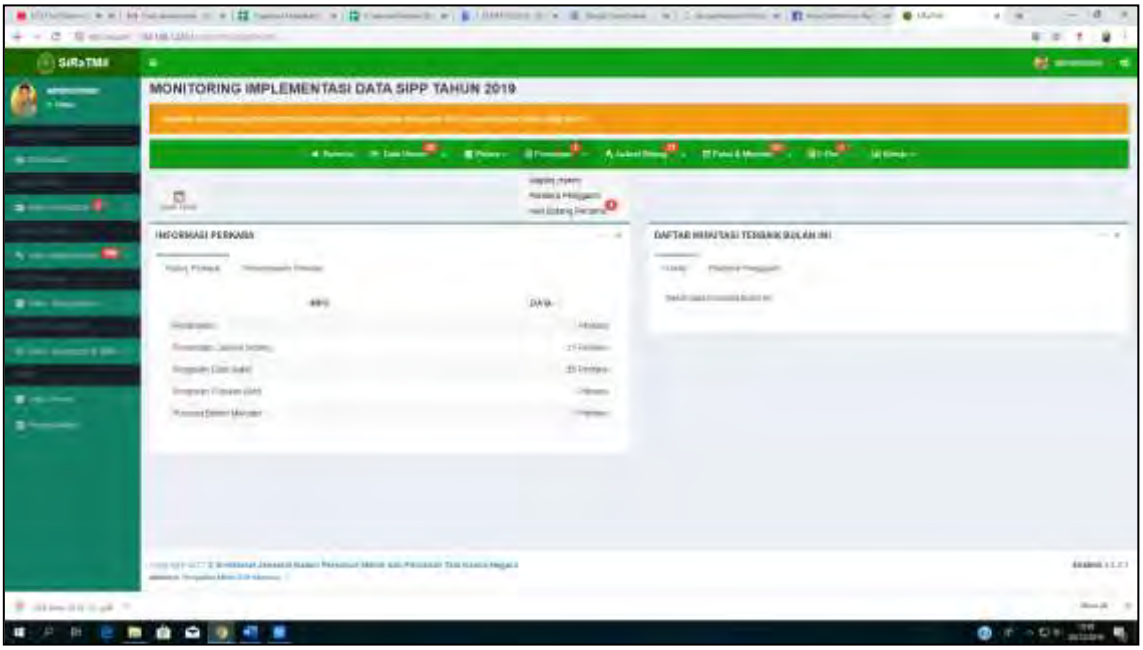




Sistem Informasi Penelususran Perkara Web

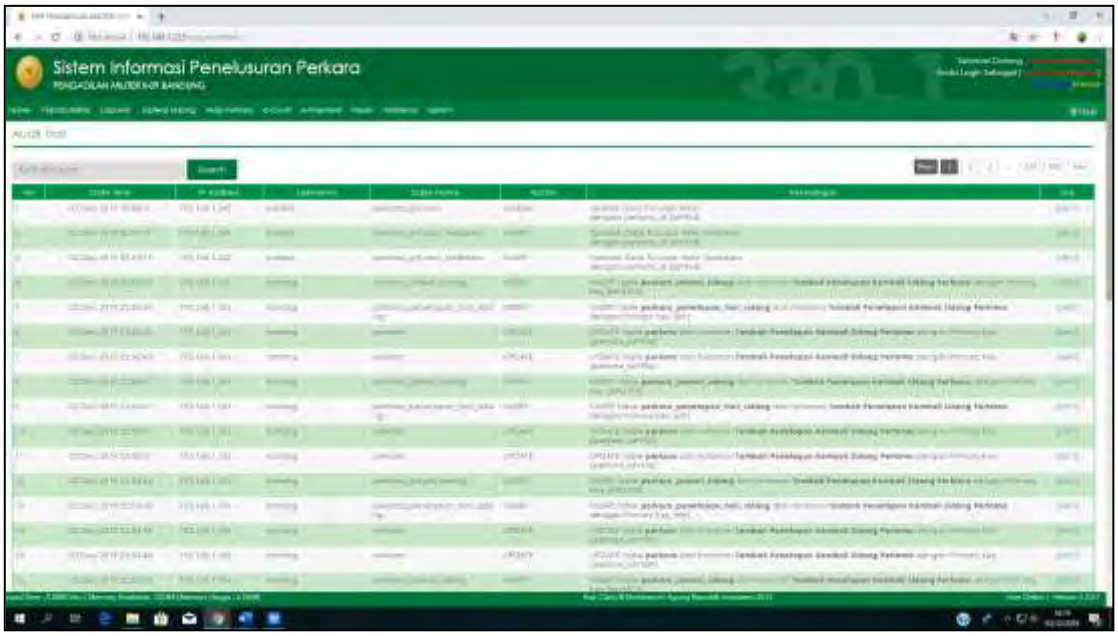


Monitoring Implementasi Data SIPP Tahun 2019

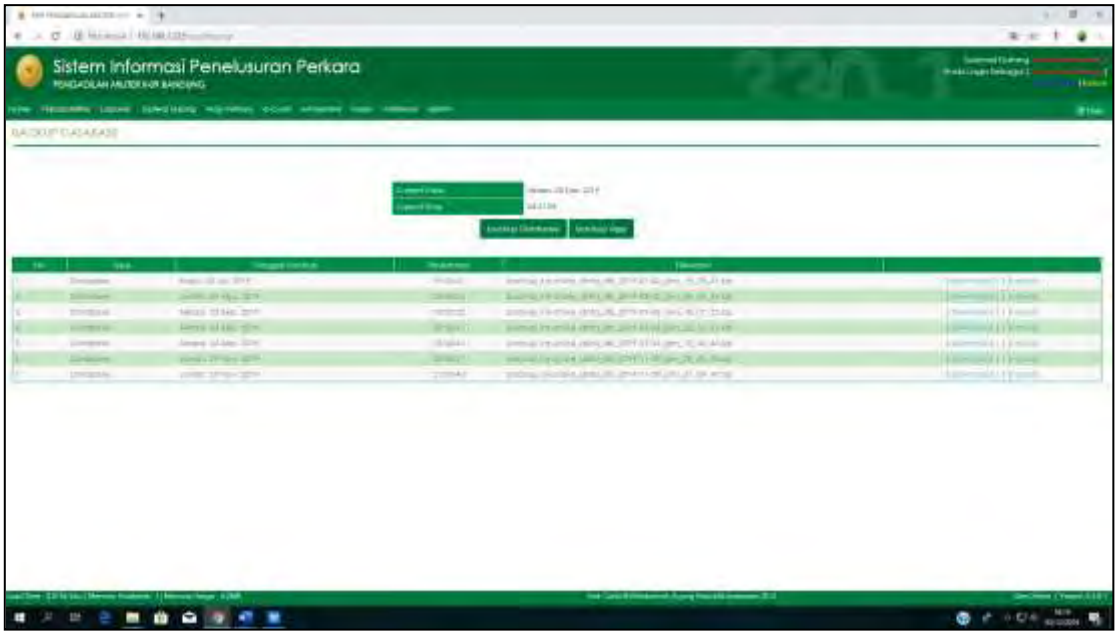


Kegiatan rutin sosialisasi dan pelatihan Sistem Informasi Penelusuran Perkara

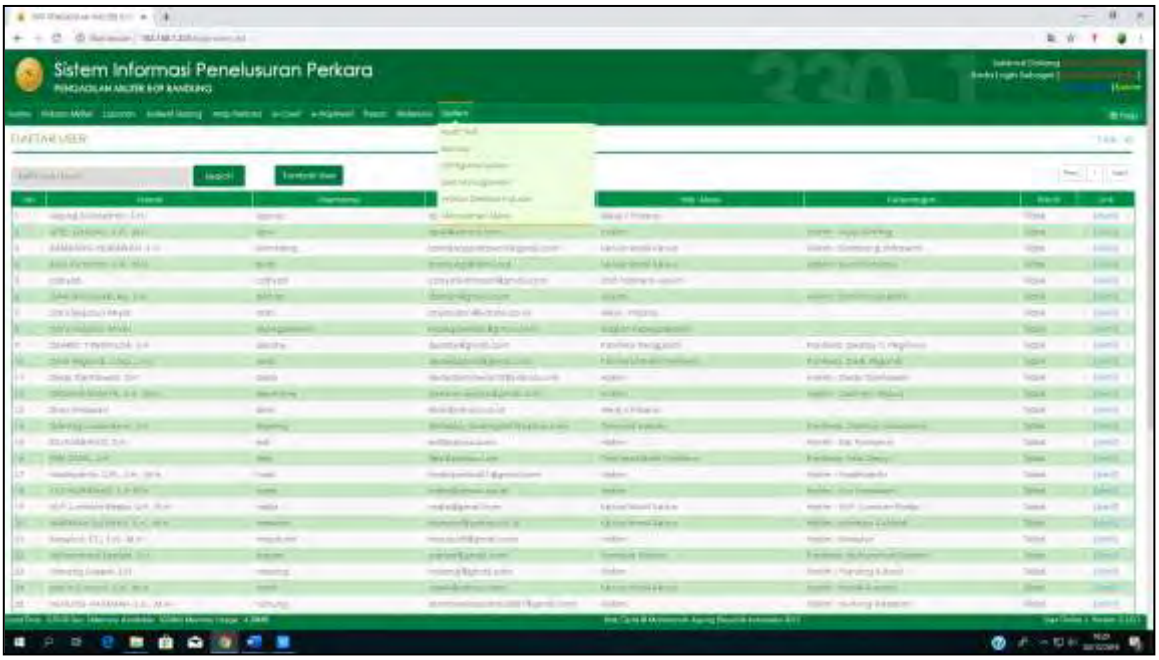
Audit Trail Sistem Informasi Penelusuran Perkara



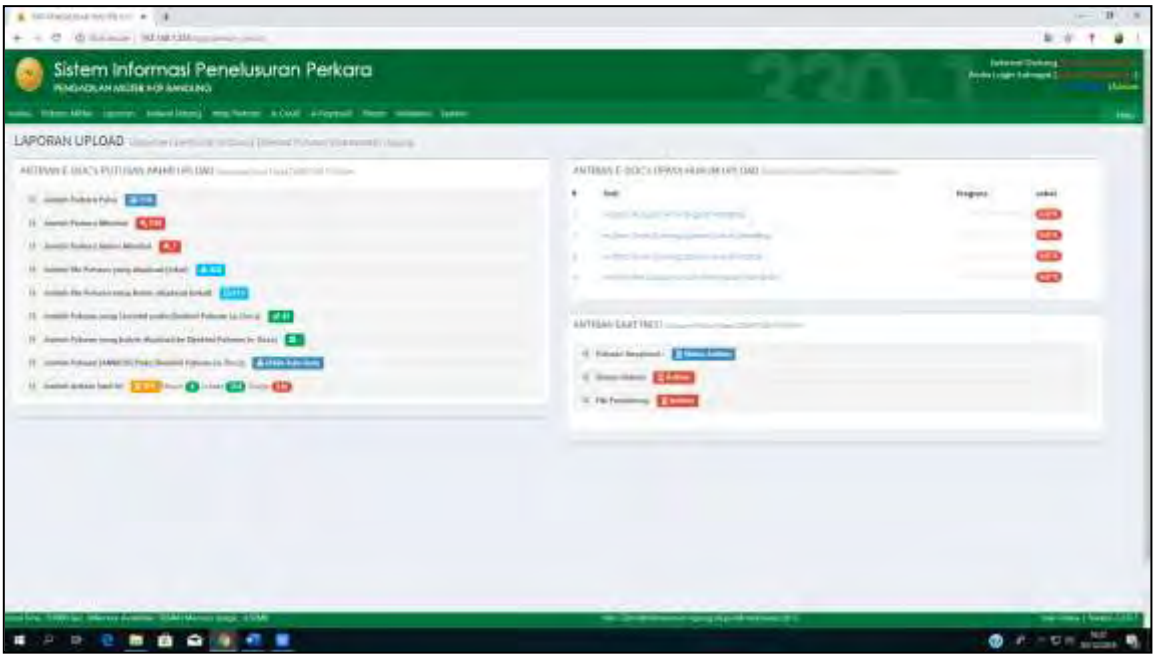
Backup database dan aplikasi Sistem Informasi Penelusuran Perkara



User Management Sistem Informasi Penelusuran Perkara



Laporan Antrian Direktori Putusan



Operator SIPP